Wireless LAN Device Series

WLAN Outdoor Bridge

AWAP08O-11gHP User Manual

Version. 1.2.1 (25.03.2005)

Table of Contents

Preface....3
Ch 1.AWAP08O-11gHP Installation....4
Packing List....4
Hardware Installation....5
Ch 2. First Time Configuration....8
Before Start to Configure....8
Knowing the Network Application....8
Advanced Settings....34
Configuring Wireless Security....37
Configuring as WLAN Client Adapter....40
Quick start to configure....40
Ch 3. Configuring WDS....43
WDS network topology....43
WDS Application....45
Ch 4. Advanced Configurations....47
Configuring LAN to WAN Firewall....47
Port Filtering....47
IP Filtering....47
MAC Filtering....47
Configuring Port Forwarding (Virtual Server)....48
Multiple Servers behind NAT Example:....49
Configuring DMZ....49
Configuring WAN Interface....50
Static IP....51
DHCP Client (Dynamic IP)....52
PPPoE....52
PPTP....53
Configuring Clone MAC Address....54
Configuring DHCP Server....57
Using CLI Menu....57
The System Management....59
About SNMP Agent....59
Firmware Upgrade....59
Configuration Data Backup & Restore....60

Preface

This guide is for the networking professional who installs and manages the Ziwell AWAP08O-11gHP outdoor product, hereafter referred to as the "device". To use this guide, you should have experience working with the TCP/IP configuration and be familiar with the concepts and terminology of wireless local area networks.

Ch 1. AWAP08O-11gHP Installation

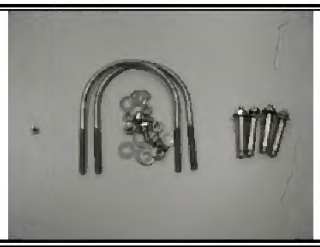
Packing List

Before you start to install the ODU, make sure the package contains the following items :

- Wireless Outdoor Bridge unit * 1
- Mounting Kit * 1
- Waterproof (IP67) RJ-45 Cable (30M) * 1
- Waterproof (IP66) RF Cable (1M) * 1
- Power Over Ethernet Kit * 1
- Ground Wire * 1
- 2.5" /4" U bolts * 2 and Anchor * 4
- 6 dBi omni directional antenna * 1 (separated package)
- RJ-45 Cable (1.5M) * 1

Outdoor unit_(ODU)	Power Over Ethernet Kit

2.5" /4" U bolt and Anchor



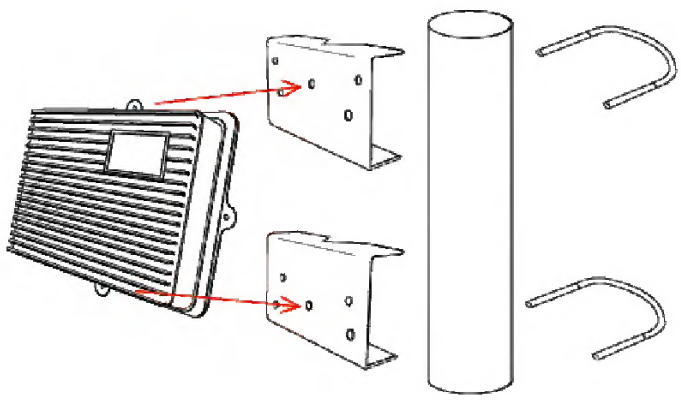
Hardware Installation

Once you check off everything from the package, you can start to install the ODU. You can mount to a pipe, a pole or to the side of a building. The steps are showed in the following :

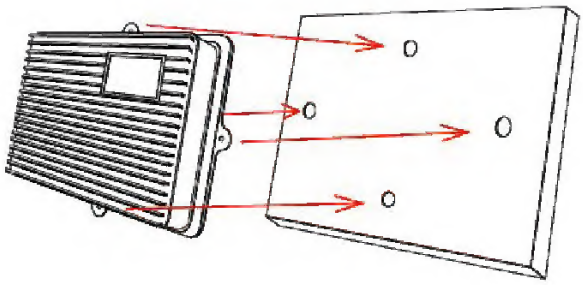
1. You must mount the ODU into the bracket first.

Note: ALL the 4 screws had been tightened onto the ODU and bracket

2. You can use the 2 or 4 inches U bolt to mount on the pipe, depending on the radius of the pipe. (Wall mounting is referred to Wall Mounting Figure) The two U bolts must be mounted tightly. Be aware of not over-tighten the U bolt.



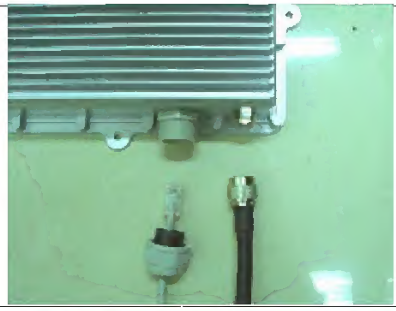
Pipe Mounting Figure



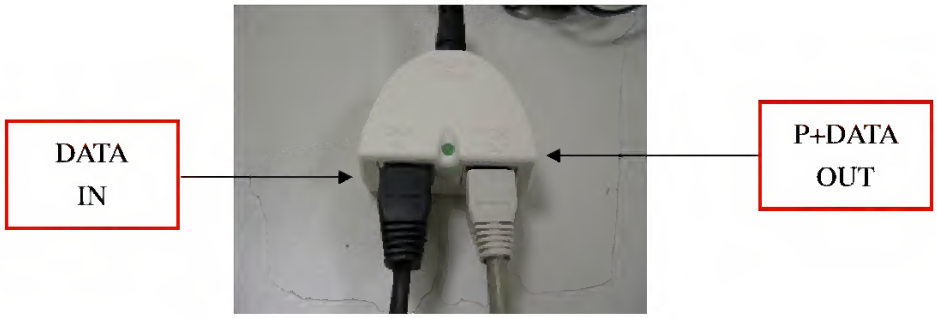
Wall Mounting Figure

3. After checking the ODU is mounted well, you can connect the following two cables: the Waterproof RJ-45 network cable to "P+ DATA OUT" port of ODU and the RF cable to antenna port. Additional waterproof tool, such as waterproof tape, is recommended to use to enhance the waterproof function. It is suggested to have a lightening protector between antenna and antenna port. Connecting the ground wire as the figure of "ODU ground wire connection."

AWAP08O-11gHP Cable Connection



4. Plug the other end of the waterproof RJ-45 cable to the PoE device. The PoE device is guaranteed only in indoor environment.



Caution: DON'T plug the power cord into PoE device before you finish install the antenna and Ground wire to ensure the safety.

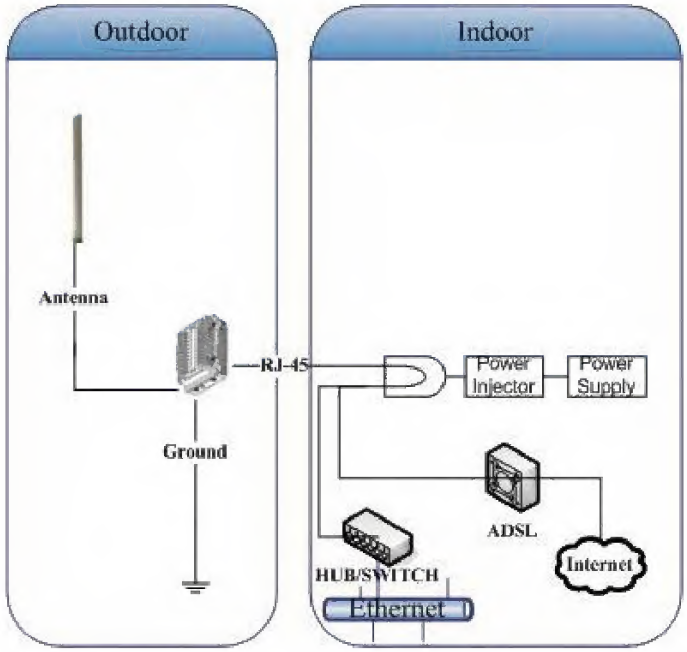
If the RJ-45 cable's length is not long enough to connect to your network device for indoor parts installation, you can extend the cable length. However, make sure the maximum length of the RJ-45 cable is shorter than 100M (about 109 yards) for normal operation under IEEE 802.3 standards.

When you plug the regular RJ-45 cable into the PoE device, you should use the regular RJ-45 cable to plug into the "DATA IN" of "Power Over Ethernet Kit" to connect to hub/switch or use the crosslink RJ-45 cable (Not included in the Packing List) to connect with user's PC.

The waterproof RJ-45 cable must be connected to the "P+DATA OUT" port.

Caution: Be careful! Don't plug the two cables inversely. It will damage the devices!

We recommend you refer to the following illustration as a guideline for hardware installation.



Ch 2. First Time Configuration

Before Start to Configure

There are two interfaces to configure the device, one is web-browser interface, and the other is Secure Shell CLI interface. To access the configuration interfaces, make sure you are using a computer connected to the same network as the device. The default IP address of the device is 192.168.2.254, and the subnet-mask is 255.255.255.0.

The device has three operation modes (Router/Bridge/WISP). In bridge mode, you can access the device by both WLAN (Wireless Local Area Network) and wired LAN. And in router/WISP modes, the device can be accessed by both WLAN and WAN. The default IP addresses for the device are 192.168.2.254(for LAN), 172.1.1.1(for WAN), so you need to make sure the IP address of your PC is in the same subnet as the device, such as 192.168.2.X(for LAN), 172.1.1.X(for WAN).

Please note that the DHCP server inside the device is default to up and running. Do not have multiple DHCP servers in your subnet, otherwise it will cause abnormal situation.

Inside the CD, we provide the device auto-discovery tool, the tool can detect the device even your PC is not in the same subnet as the device in case the IP address of device is changed and forgot by user. The tool only can discover the device in your local area network.

Knowing the Network Application

ZWA-G192-OD can act as the following roles, and it supports WDS (Wireless Distribution System) function.

- Access Point
- WDS (Wireless Repeater)
- Bridge/Router
- WISP
- AP Client

The device provides 3 different operation modes and the wireless radio of device can act as AP/Client/WDS. The operation mode is about the communication mechanism between the wired Ethernet NIC and wireless NIC, the following is the types of operation mode.

Router

The wired Ethernet (WAN) port is used to connect with ADSL/Cable modem and the wireless NIC is used for your private WLAN. The NAT is existed between the 2 NIC and all the wireless clients share the same public IP address through the WAN port to ISP. The default IP configuration for WAN port is static IP. You can access the web server of device through the default WAN IP address 172.1.1.1 and modify the setting base on your ISP requirement.

Bridge

The wired Ethernet and wireless NIC are bridged together. Once the mode is selected, all the WAN related functions will be disabled.

WISP (Wireless ISP)

This mode can let you access the AP of your wireless ISP and share the same public IP address form your ISP to the PCs connecting with the wired Ethernet port of the device. To use this mode, first you must set the wireless radio to be client mode and connect to the AP of your ISP then you can configure the WAN IP configuration to met your ISP requirement.

The wireless radio of the device acts as the following roles.

AP (Access Point)

The wireless radio of device serves as communications "hub" for wireless clients and provides a connection to a wired LAN.

AP Client

This mode provides the capability to connect with the other AP using infrastructure/Ad-hoc networking types. With bridge operation mode, you can directly connect the wired Ethernet port to your PC and the device becomes a wireless adapter. And with WISP operation mode, you can connect the wired Ethernet port to a hub/switch and all the PCs connecting with hub/switch can share the same public IP address from your ISP.

WDS (Wireless Distribution System)

This mode serves as a wireless repeater, the device forwards the packets to another AP with WDS function. When this mode is selected, all the wireless clients can't

survey and connect to the device. The device only allows the WDS connection.

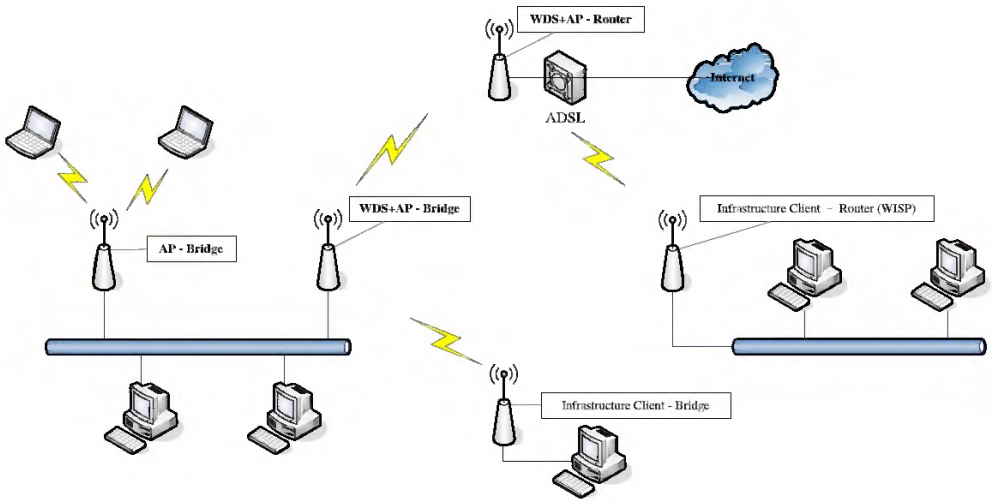
WDS+AP

This mode combines WDS plus AP modes, it not only allows WDS connections but also the wireless clients can survey and connect to the device.

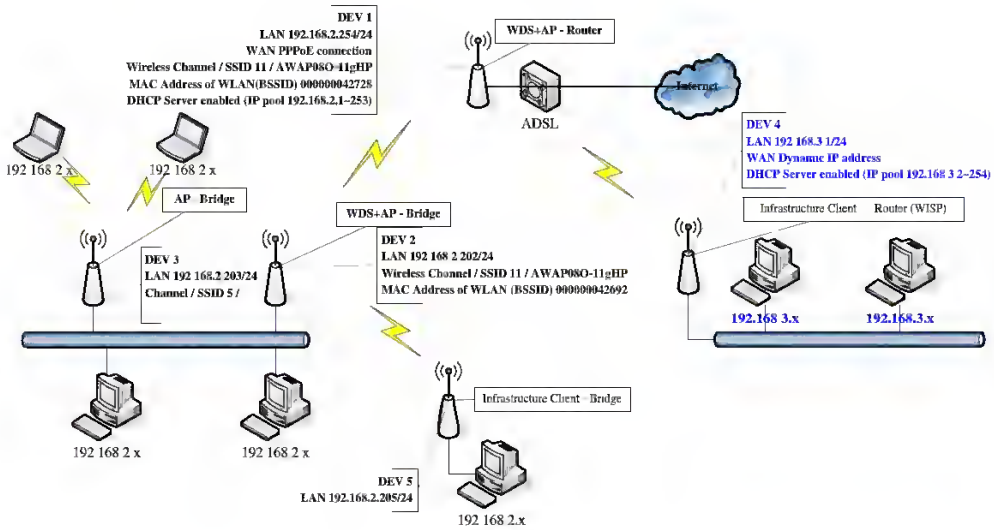
The following table shows the supporting combination of operation and wireless radio modes.

	Bridge	*Router*	*WISP*
AP	V	v	x
WDS	V	v	x
Client	v	x	v
AP+WDS	v	v	x

Hereafter are some topologies of network application for your reference.



Examples of Configuration



This example demonstrates how to set up a network with different device configurations. There are 2 DHCP servers (DEV1/DEV4) in the network to control the IP configuration of 2 domains (192.168.2.x/192.168.3.x). Once the setting is done, all the PCs can visit Internet through DEV1.

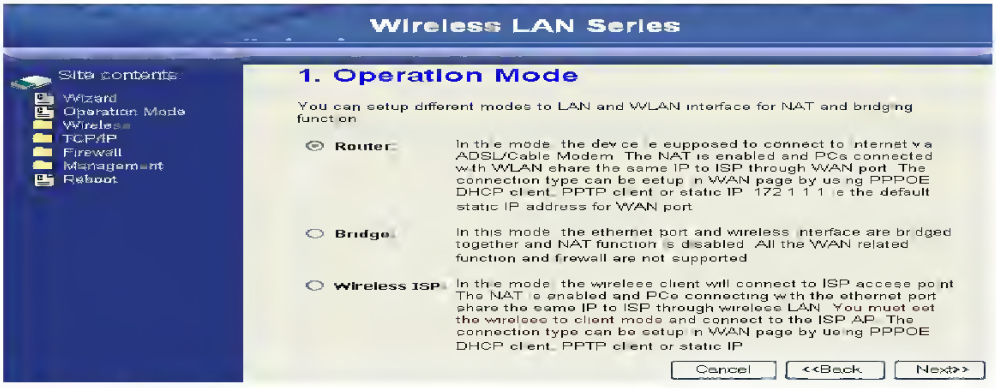
We assume all the devices keep the factory default setting. To make sure that user can continuing press the rest button for more than 5 seconds to restore the factory default setting.

The following descriptions show the steps to configure DEV1 to DEV5.

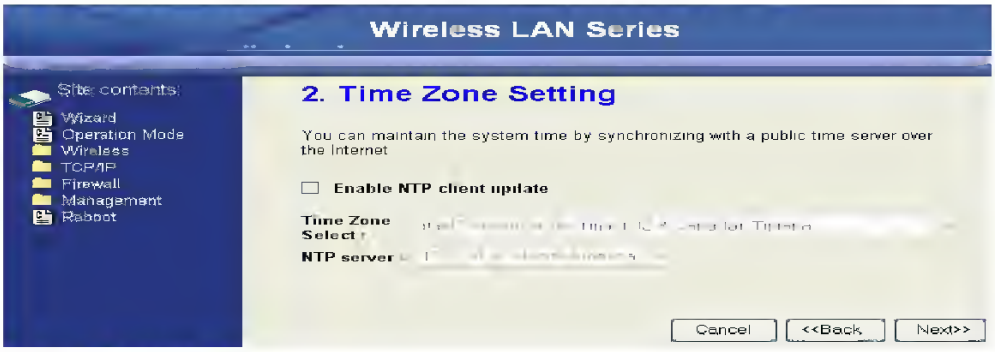
Configure DEV1:

1. Connect the ADSL modem to Ethernet port of device using Ethernet cable.
2. Access the web server (http://192.168.2.254) of device from the wireless station.
3. Use Wizard page to setup device.

4. Press "Next>>" button then set the "Operation Mode" to "Router" mode.



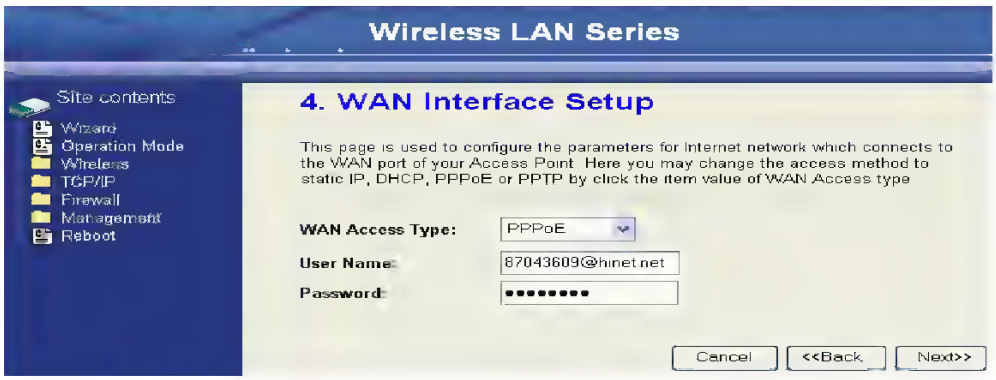
5. Press "Next>>" button then disable "Time Zone" function.



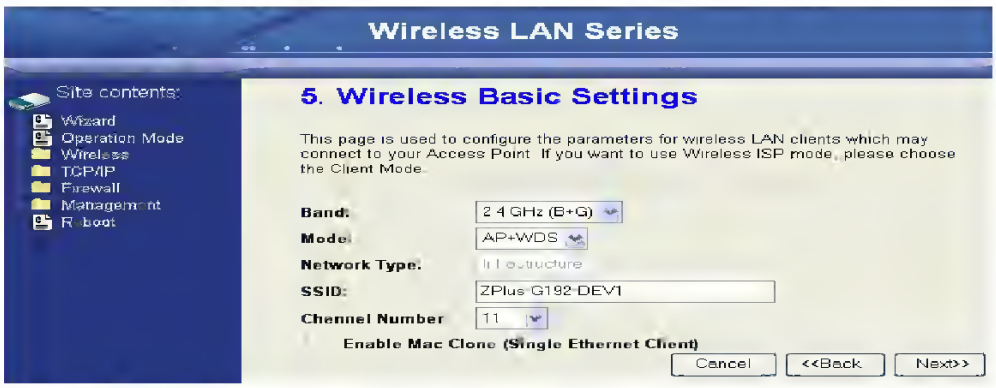
6. Press "Next>>" button then set the IP address of LAN interface.

Wireless LAN Series
Site contents:
Wizard
Operation Mode
Wireless
TCP/IP
Firewall
Management
Reboot
3. LAN Interface Setup
This page is used to configure the parameters for local area network which connects to the device. Here you may change the setting for IP addresss, subnet mask. The DHCP Server will be up and running, please make sure there is no another DHCP Server in your network when the device is in Bridge/Client Modes.
IP Address:
192.168.2.254
Subnet Mask:
255.255.255.0
Cancel
<<Back
Next>>

7. Press “Next>>” button then select the “PPPoE” for “WAN Access Type” and fill in the “User Name” and “Password” fields.

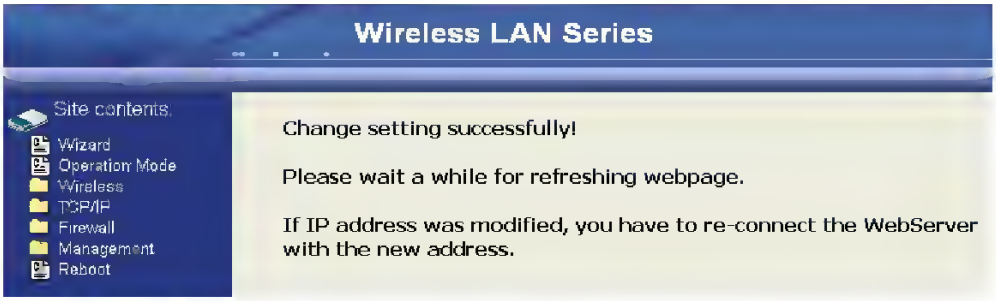


8. Press “Next>>” button then select the “AP+WDS” for “mode” and change the SSID to “AWAP08O-11gHP”.

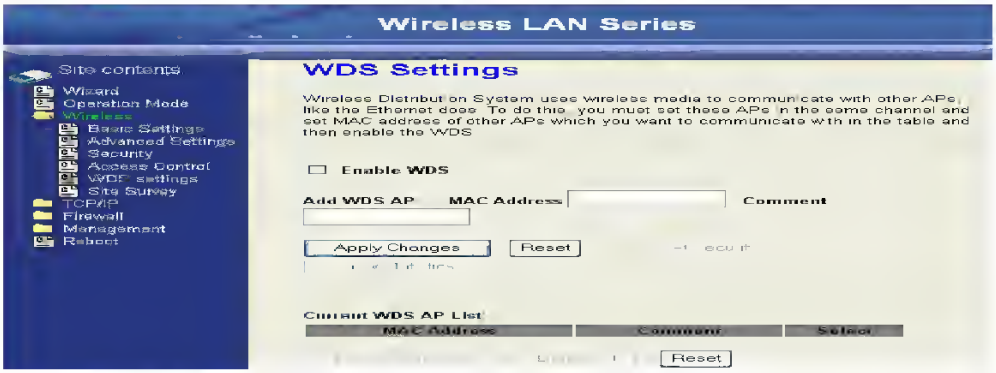


9. Press “Next>>” button then select “None” for “Encryption” then press “Finished” button.

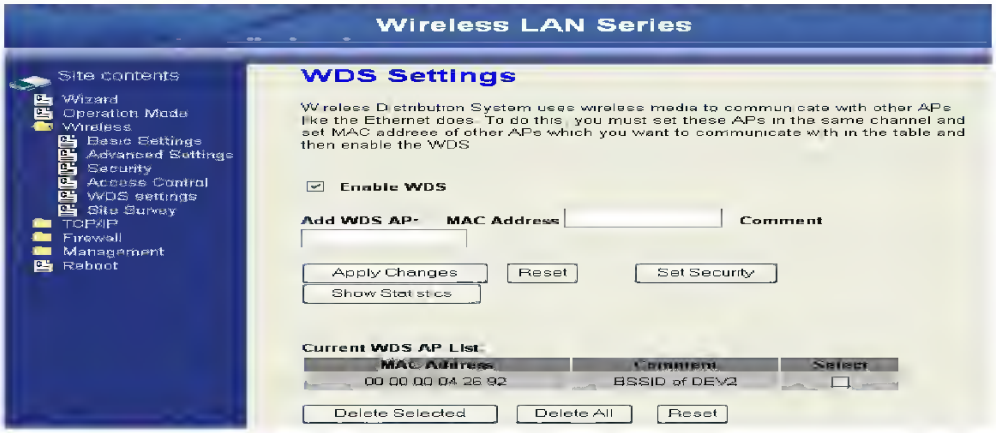
10. Wait for refreshing web page.



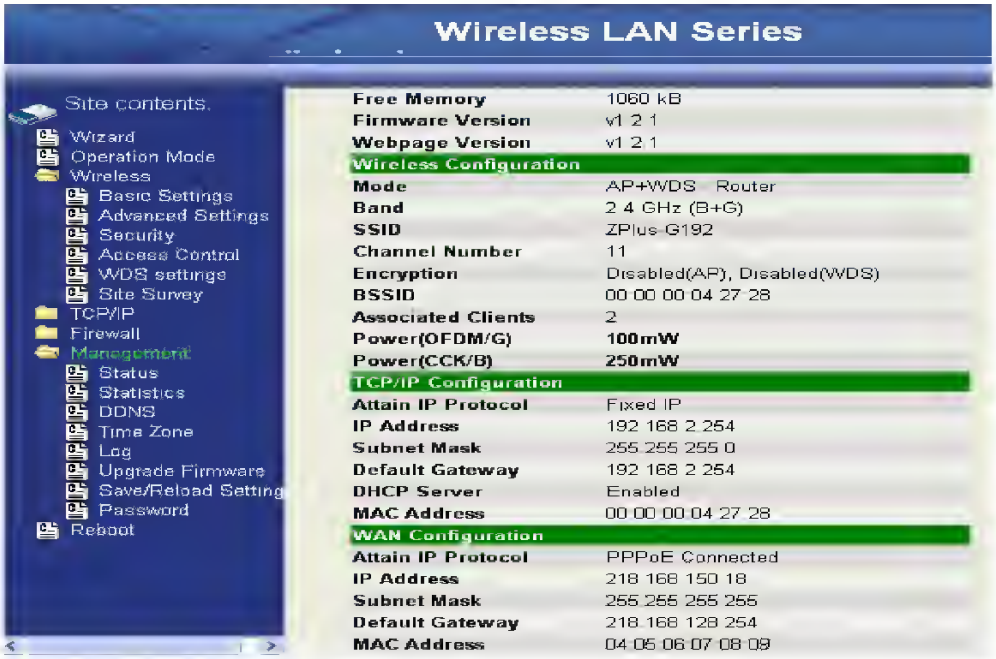
11. Use "WDS Settings" page to configure WDS.



12. Enable WDS function and add the BSSID of DEV2 to "Current WDS AP List".



13. Since we access the device by wireless connection, it may temporarily disconnect when applying the WDS setting. After re-connecting to the device, use the "Status " page to check the settings.



Configure DEV2:

1. Access the web server (http://192.168.2.254) of device from the Ethernet port.

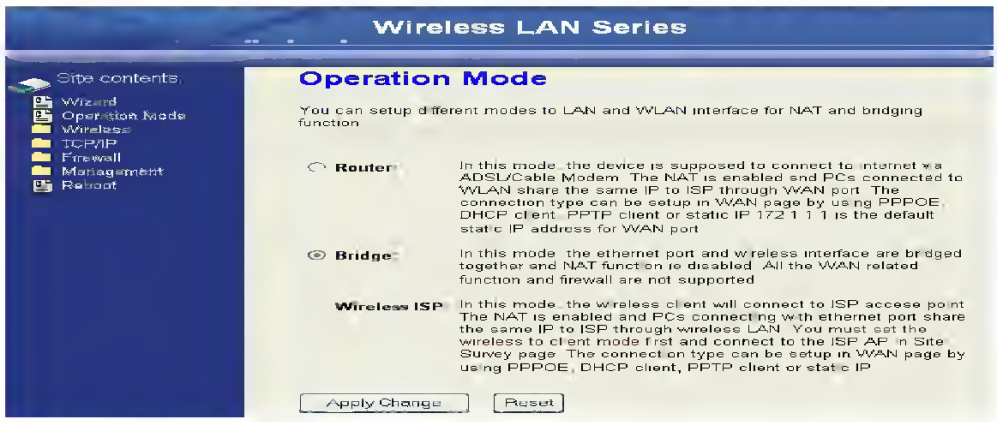
Caution

If you configure multiple devices in the same PC, since the devices have the same default IP address but different MAC addresses, it may cause you can't access the web server of device. If the situation happens, please try to clean the ARP table of your PC by DOS command "arp –d" then you can access the web server of device using the default IP address.

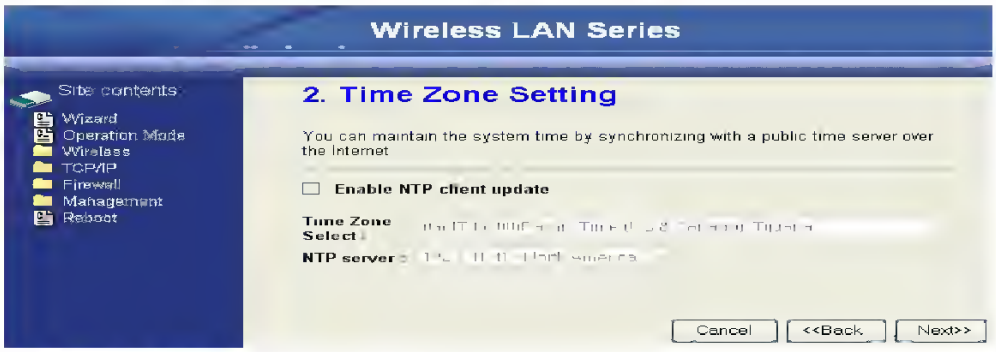
2. Use Wizard page to setup device.

Zinwell WLAN AP Webserver
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.2.254/home.asp
Wireless LAN Series
Site contents
Wizard
Operation Mode
Wireless
TCP/IP
Firewall
Management
Reboot
Setup Wizard
The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by step.
Welcome to Setup Wizard.
The Wizard will guide you the through following steps. Begin by clicking on Next.
1 Setup Operation Mode
2 Choose your Time Zone
3 Setup LAN Interface
4 Setup WAN Interface
5 Wireless LAN Setting
6 Wireless Security Setting
Next>>

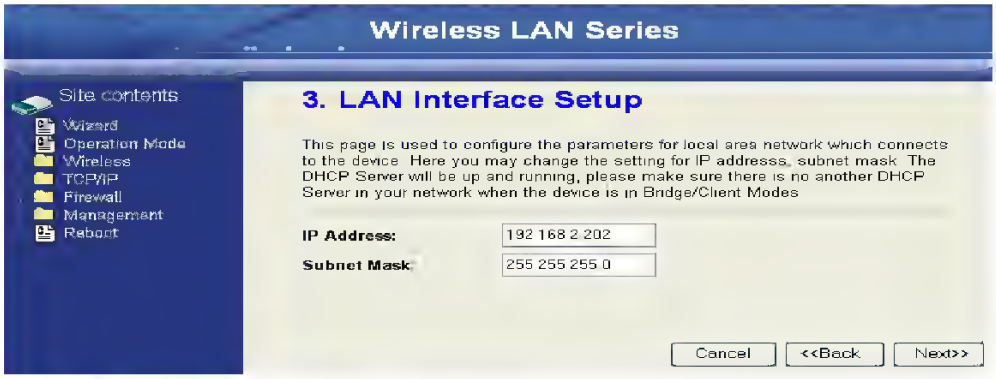
3. Press "Next>>" button then set the "Operation Mode" to "Bridge" mode.


Wireless LAN Series
Site contents:
Wizard
Operation Mode
Wireless
TCP/IP
Firewall
Management
Reboot
Operation Mode
You can setup different modes to LAN and WLAN interface for NAT and bridging function.
Router: In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs connected to WLAN share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP. 172.1.1.1 is the default static IP address for WAN port.
Bridge: In this mode, the ethernet port and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
Wireless ISP: In this mode, the wireless client will connect to ISP access point. The NAT is enabled and PCs connecting with ethernet port share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.
Apply Change
Reset

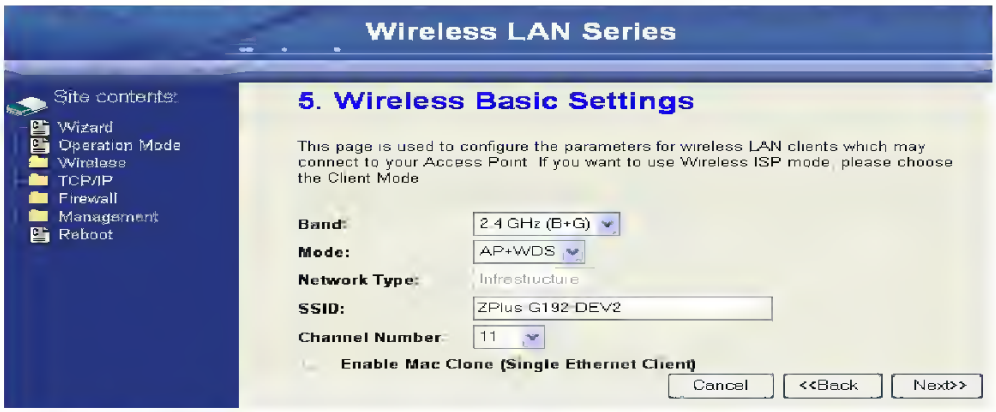
4. Press "Next>>" button then disable "Time Zone" function.



5. Press "Next>>" button then set the IP address of LAN interface.

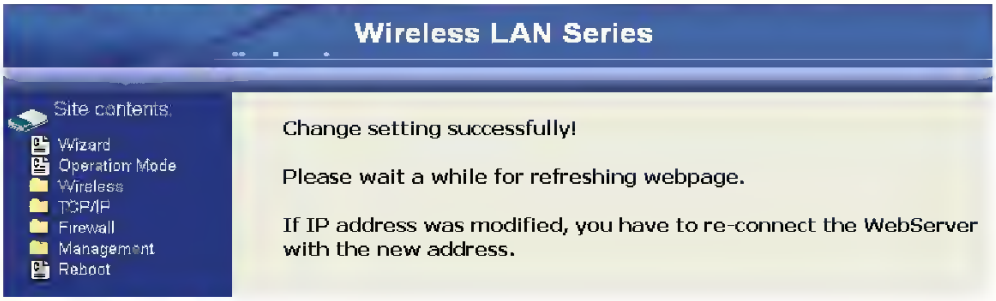

Wireless LAN Series
Site contents:
Wizard
Operation Mode
Wireless
TCP/IP
Firewall
Management
Reboot
3. LAN Interface Setup
This page is used to configure the parameters for local area network which connects to the device. Here you may change the setting for IP addresss, subnet mask. The DHCP Server will be up and running, please make sure there is no another DHCP Server in your network when the device is in Bridge/Client Modes
IP Address:
192.168.2.202
Subnet Mask:
255.255.255.0
Cancel
<<Back
Next>>

6. Press "Next>>" button then select the "AP+WDS" for "mode" and change the SSID to "AWAP08O-11gHP".

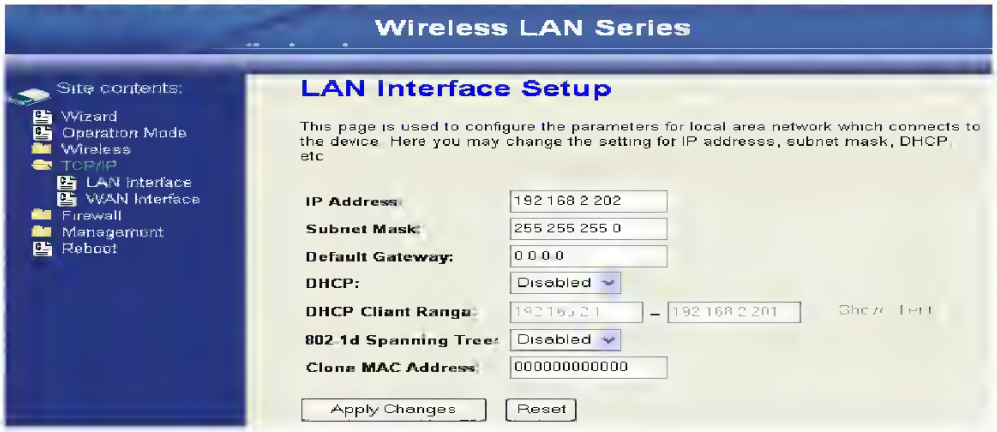


7. Press "Next>>" button then select "None" for "Encryption" then press "Finished" button.

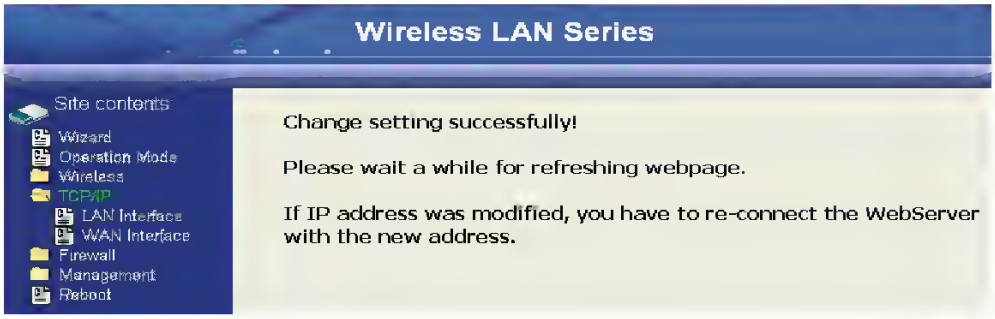
8. Wait for refreshing web page.



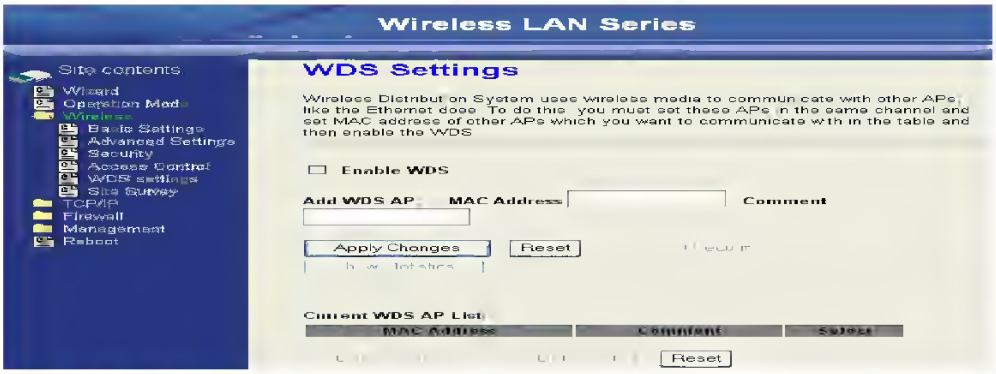
9. Access the web server by new IP address "192.168.2.202" then use "LAN Interface" page to disable DHCP Server.



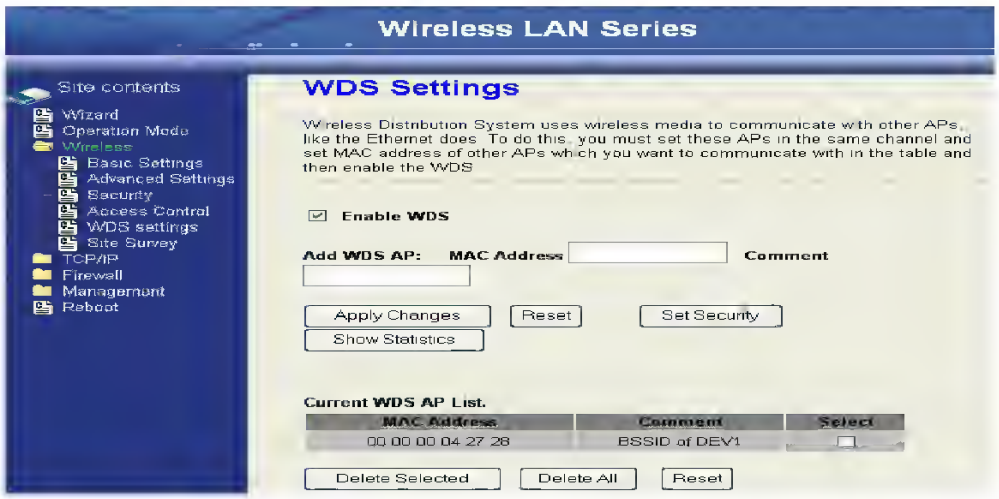
10. Wait for refreshing web page.



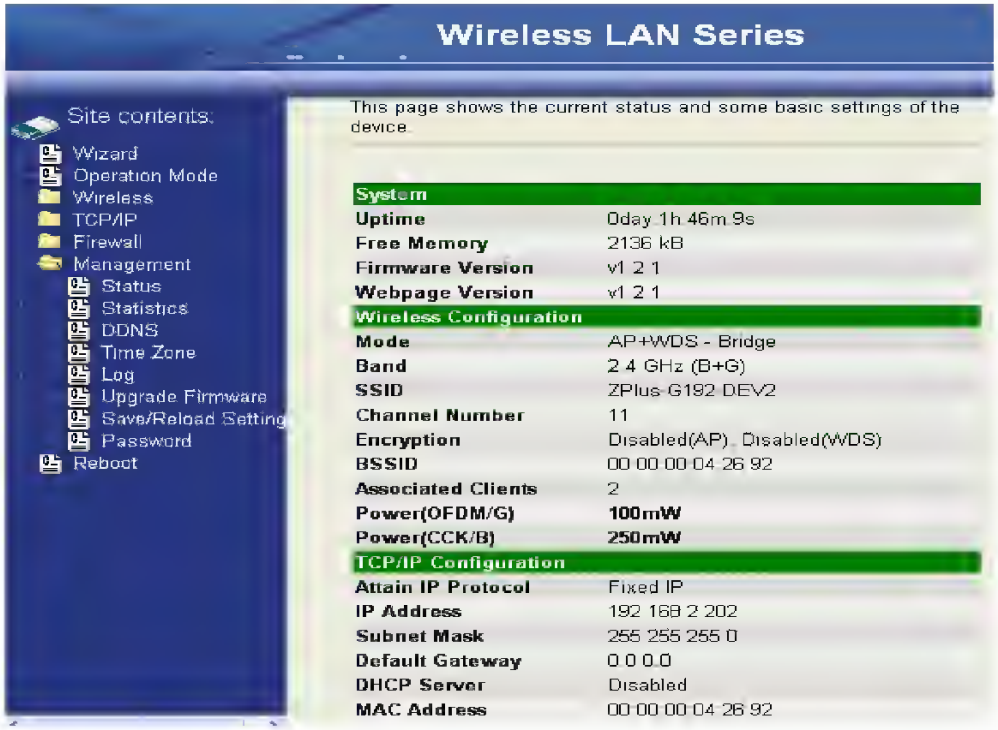
11. Use "WDS Settings" page to configure WDS.



12. Enable WDS function and add the BSSID of DEV1 to "Current WDS AP List".



13. Use the "Status " page to check the settings.


Wireless LAN Series
Site contents:
Wizard
Operation Mode
Wireless
TCP/IP
Firewall
Management
Status
Statistics
DDNS
Time Zone
Log
Upgrade Firmware
Save/Reload Setting
Password
Reboot
This page shows the current status and some basic settings of the device.
System
Uptime 0day:1h:46m:9s
Free Memory 2136 kB
Firmware Version v1.2.1
Webpage Version v1.2.1
Wireless Configuration
Mode AP+WDS - Bridge
Band 2.4 GHz (B+G)
SSID ZPlus-G192 DEV2
Channel Number 11
Encryption Disabled(AP), Disabled(WDS)
BSSID 00:00:00:04:26:92
Associated Clients 2
Power(OFDM/G) 100mW
Power(CCK/B) 250mW
TCP/IP Configuration
Attain IP Protocol Fixed IP
IP Address 192.168.2.202
Subnet Mask 255.255.255.0
Default Gateway 0.0.0.0
DHCP Server Disabled
MAC Address 00:00:00:04:26:92

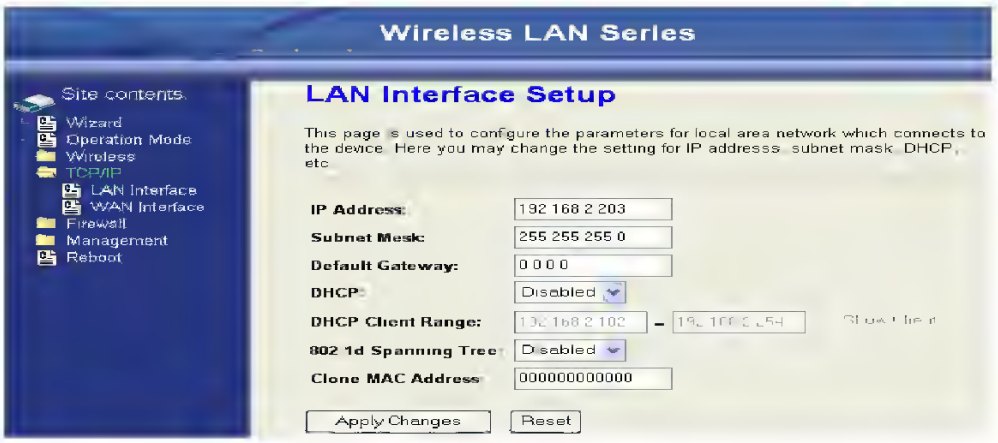
Configure DEV3:

1. Access the web server (http://192.168.2.254) of device from the Ethernet port.

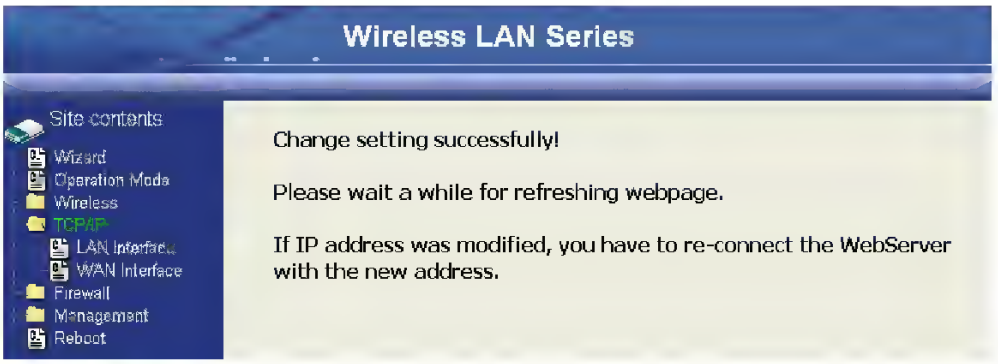
Caution

If you configure multiple devices in the same PC, since the devices have the same default IP address but different MAC addresses, it may cause you can't access the web server of device. If the situation happens, please try to clean the ARP table of your PC by DOS command "arp –d" then you can access the web server of device using the default IP address.

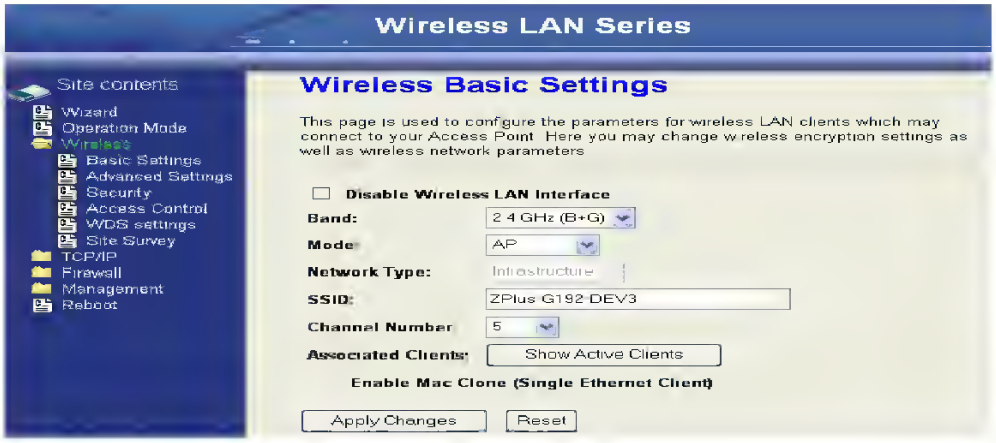
2. Use "LAN Interface" page to set the IP address of LAN interface and disable DHCP server.



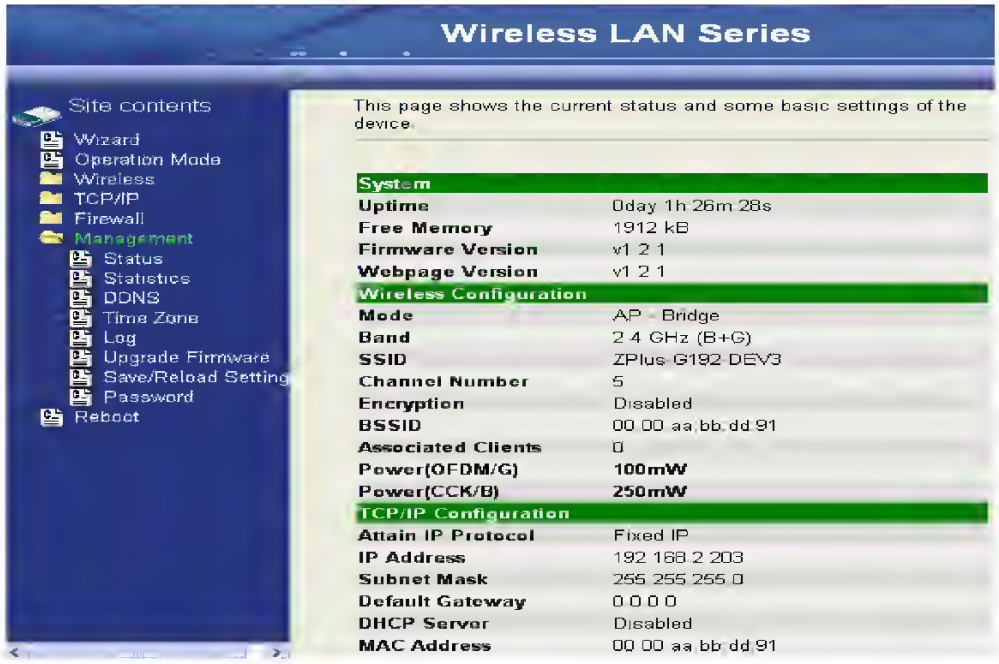
3. Wait for refreshing web page.



4. Access the web server by new IP address "192.168.2.203" then use "Basic Settings" page to change SSID and CHANNEL.



5. Use the "Status " page to check the settings.



Configure DEV4:

1. Access the web server (http://192.168.2.254) of device from the Ethernet port.

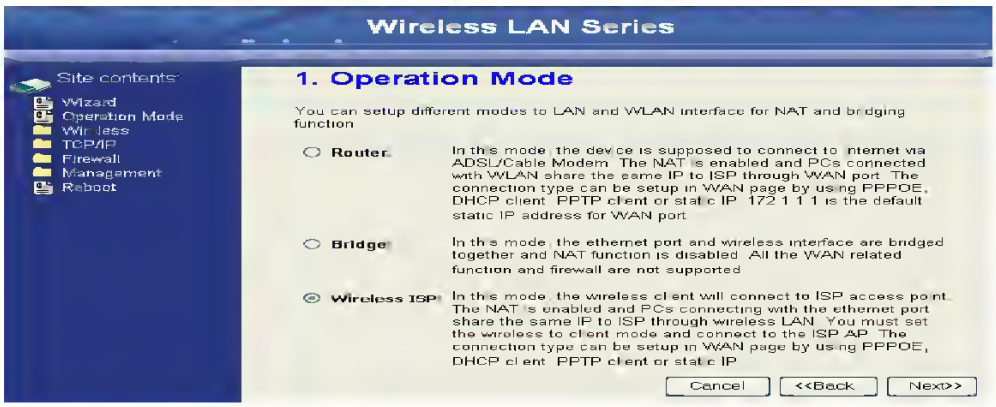
Caution

If you configure multiple devices in the same PC, since the devices have the same default IP address but different MAC addresses, it may cause you can't access the web server of device. If the situation happens, please try to clean the ARP table of your PC by DOS command "arp –d" then you can access the web server of device using the default IP address.

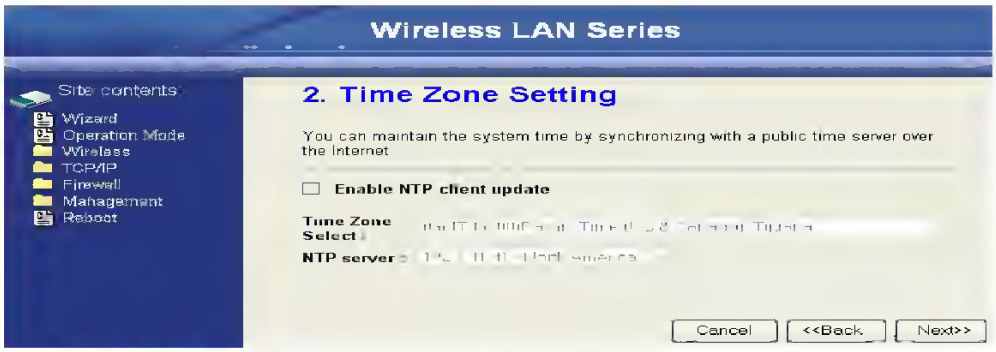
2. Use Wizard page to setup device.

Zinwell WLAN AP Webserver
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.2.254/home.asp
Wireless LAN Series
Site contents
Wizard
Operation Mode
Wireless
TCP/IP
Firewall
Management
Reboot
Setup Wizard
The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by step.
Welcome to Setup Wizard.
The Wizard will guide you the through following steps. Begin by clicking on Next.
1 Setup Operation Mode
2 Choose your Time Zone
3 Setup LAN Interface
4 Setup WAN Interface
5 Wireless LAN Setting
6 Wireless Security Setting
Next>>

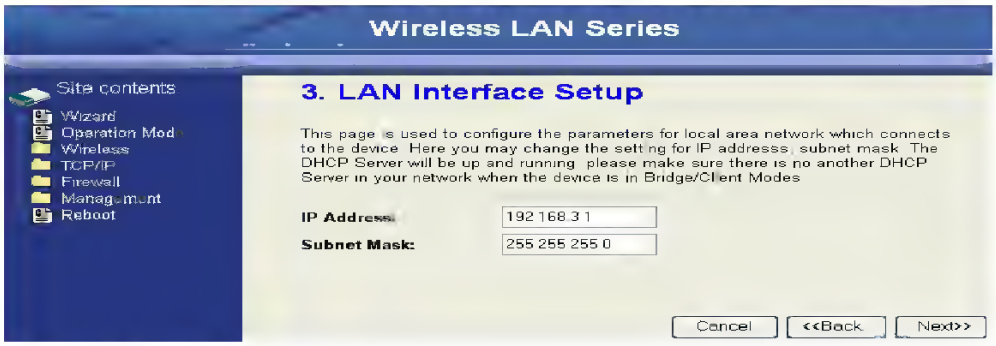
3. Press "Next>>" button then set the "Operation Mode" to "Wireless ISP" mode.


Wireless LAN Series
Site contents
Wizard
Operation Mode
Wireless
TCP/IP
Firewall
Management
Reboot
1. Operation Mode
You can setup different modes to LAN and WLAN interface for NAT and bridging function.
Router: In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs connected with WLAN share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP. 172.1.1.1 is the default static IP address for WAN port.
Bridge: In this mode, the ethernet port and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
Wireless ISP: In this mode, the wireless client will connect to ISP access point. The NAT is enabled and PCs connecting with the ethernet port share the same IP to ISP through wireless LAN. You must set the wireless to client mode and connect to the ISP AP. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.
Cancel <<Back Next>>

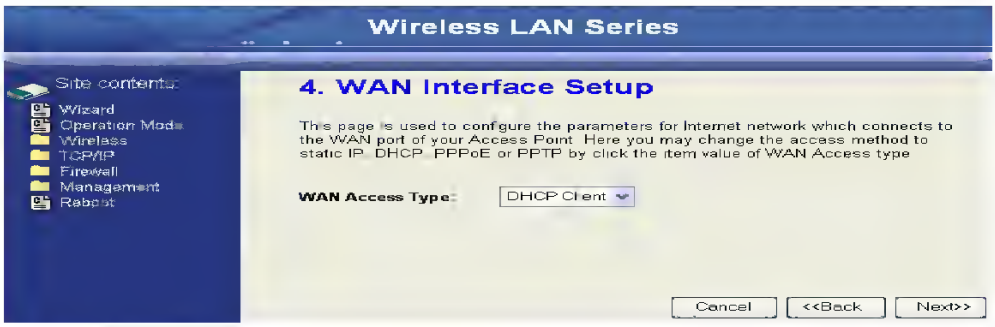
4. Press "Next>>" button then disable "Time Zone" function.



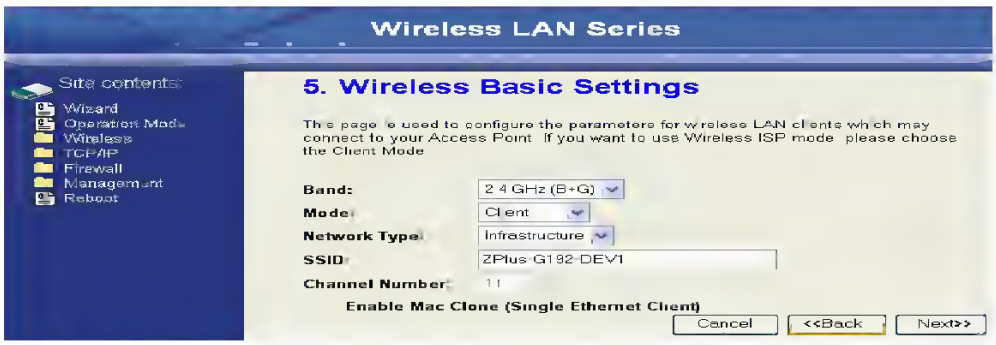
5. Press “Next>>” button then set the IP address of LAN interface.


Wireless LAN Series
Site contents:
Wizard
Operation Mod
Wireless
TCP/IP
Firewall
Managment
Reboot
3. LAN Interface Setup
This page is used to configure the parameters for local area network which connects to the device. Here you may change the setting for IP addresss, subnet mask. The DHCP Server will be up and running, please make sure there is no another DHCP Server in your network when the device is in Bridge/Client Modes
IP Address:
192.168.3.1
Subnet Mask:
255.255.255.0
Cancel
<<Back
Next>>

6. Press “Next>>” button then select the “DHCP Client” for “WAN Access Type”.

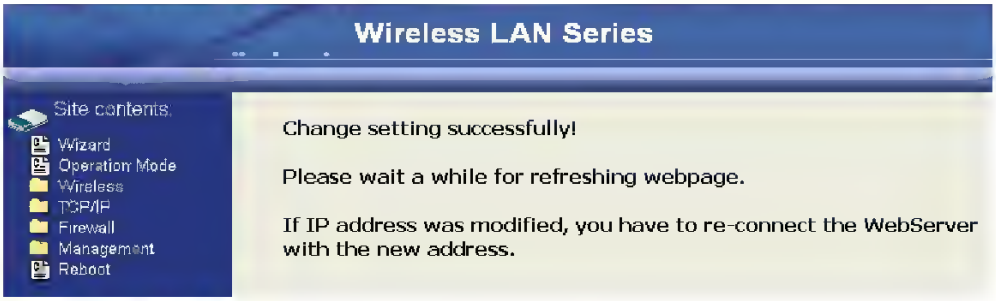

Wireless LAN Series
Site contents:
Wizard
Operation Mode
Wireless
TCP/IP
Firewall
Management
Reboot
4. WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.
WAN Access Type:
DHCP Client
Cancel
<<Back
Next>>

7. Press “Next>>” button then select the “Client” for “mode” and change the SSID to “AWAP08O-11gHP”.



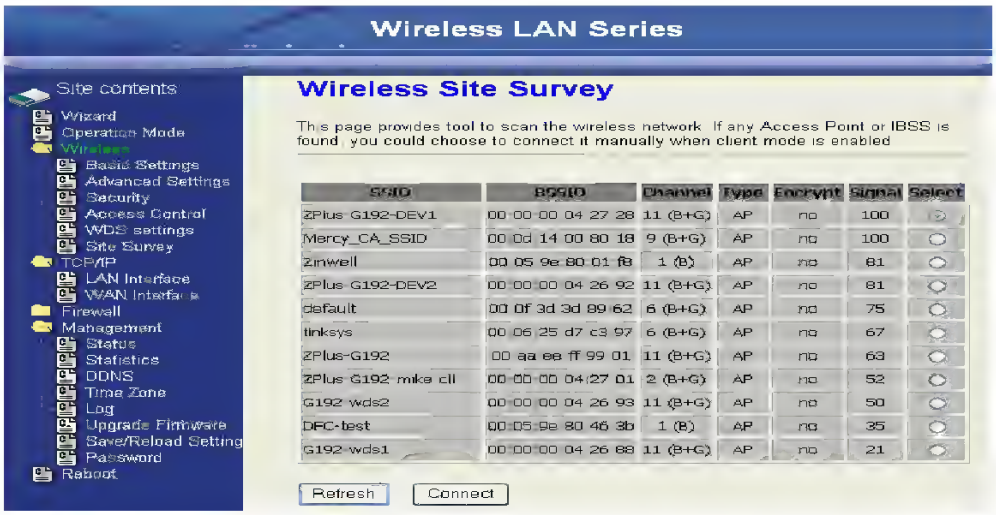
8. Press “Next>>” button then select “None” for “Encryption” then press “Finished” button.

9. Wait for refreshing web page.



10. Change the IP address of your PC to 192.168.3.x then access the web server by the new IP address "192.168.3.1" and use "Status" page check the setting.

11. If the "State" of "Wireless Configuration" is not "Connected" or you want to refresh the "RSSI ", please use "Site Survey" page to re-connect a AP.


Wireless LAN Series
Site contents
Wizard
Operation Mode
Wireless
Basic Settings
Advanced Settings
Security
Access Control
WDS settings
Site Survey
TCP/IP
LAN Interface
WAN Interface
Firewall
Management
Status
Statistics
DDNS
Time Zone
Log
Upgrade Firmware
Save/Reload Setting
Password
Reboot
Wireless Site Survey
This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.
SSID
BSSID
Channel
Type
Encrypt
Signal
Select
ZPlus-G192-DEV1 00 00 00 04 27 28 11 (B+G) AP no 100
Mercy_CA_SSID 00 0d 14 00 80 18 9 (B+G) AP no 100
Zinwell 00 05 9e 80 01 f8 1 (B) AP no 81
ZPlus-G192-DEV2 00 00 00 04 26 92 11 (B+G) AP no 81
default 00 0f 3d 3d 89 62 6 (B+G) AP no 75
linksys 00 06 25 d7 c3 97 6 (B+G) AP no 67
ZPlus-G192 00 aa 8e ff 99 01 11 (B+G) AP no 63
ZPlus-G192_mike cli 00 00 00 04 27 01 2 (B+G) AP no 52
G192-wds2 00 00 00 04 26 93 11 (B+G) AP no 50
DFC-test 00 05 9e 80 46 3b 1 (B) AP no 35
G192-wds1 00 00 00 04 26 88 11 (B+G) AP no 21
Refresh
Connect

Configure DEV5:

1. Access the web server (http://192.168.2.254) of device from the Ethernet port.

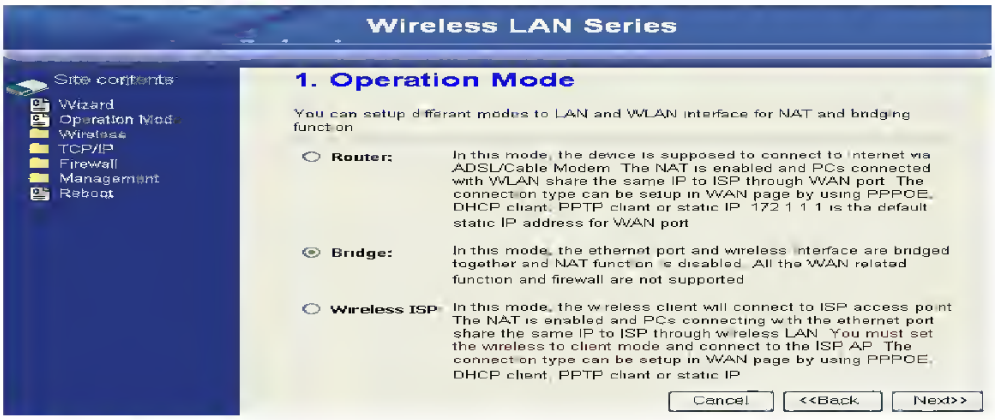
Caution

If you configure multiple devices in the same PC, since the devices have the same default IP address but different MAC addresses, it may cause you can't access the web server of device. If the situation happens, please try to clean the ARP table of your PC by DOS command "arp –d" then you can access the web server of device using the default IP address.

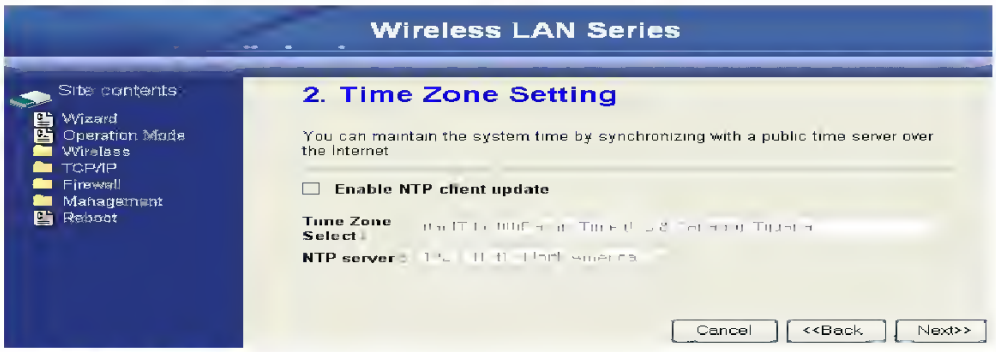
2. Use Wizard page to setup device.

Zinwell WLAN AP Webserver
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.2.254/home.asp
Wireless LAN Series
Site contents
Wizard
Operation Mode
Wireless
TCP/IP
Firewall
Management
Reboot
Setup Wizard
The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by step.
Welcome to Setup Wizard.
The Wizard will guide you the through following steps. Begin by clicking on Next.
1 Setup Operation Mode
2 Choose your Time Zone
3 Setup LAN Interface
4 Setup WAN Interface
5 Wireless LAN Setting
6 Wireless Security Setting
Next>>

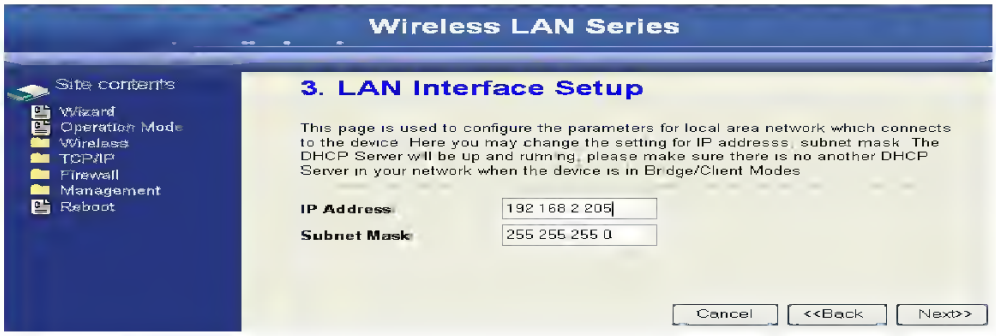
3. Press "Next>>" button then set the "Operation Mode" to "Wireless ISP" mode.


Wireless LAN Series
Site contents
Wizard
Operation Mode
Wireless
TCP/IP
Firewall
Management
Reboot
1. Operation Mode
You can setup different modes to LAN and WLAN interface for NAT and bridging function.
Router: In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs connected with WLAN share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP. 172.1.1.1 is the default static IP address for WAN port.
Bridge: In this mode, the ethernet port and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
Wireless ISP: In this mode, the wireless client will connect to ISP access point. The NAT is enabled and PCs connecting with the ethernet port share the same IP to ISP through wireless LAN. You must set the wireless to client mode and connect to the ISP AP. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.
Cancel <<Back Next>>

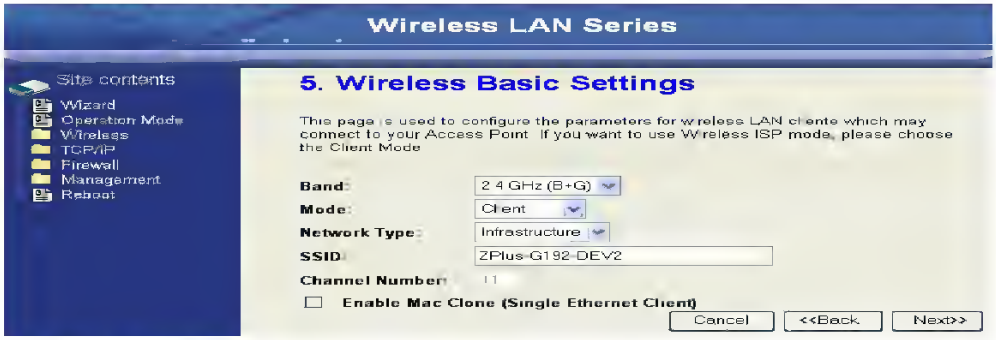
4. Press "Next>>" button then disable "Time Zone" function.



5. Press "Next>>" button then set the IP address of LAN interface.

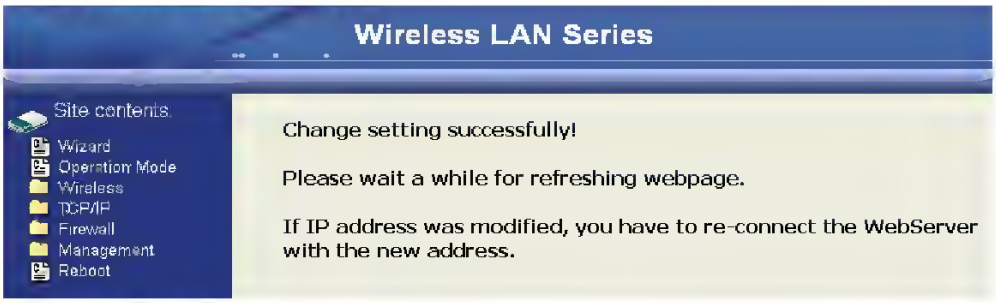

Wireless LAN Series
Site contents:
Wizard
Operation Mode
Wireless
TCP/IP
Firewall
Management
Reboot
3. LAN Interface Setup
This page is used to configure the parameters for local area network which connects to the device. Here you may change the setting for IP addresss, subnet mask. The DHCP Server will be up and running, please make sure there is no another DHCP Server in your network when the device is in Bridge/Client Modes
IP Address:
192.168.2.205
Subnet Mask:
255.255.255.0
Cancel
<<Back
Next>>

6. Press "Next>>" button then select the "Client" for "mode" and change the SSID to "AWAP08O-11gHP".

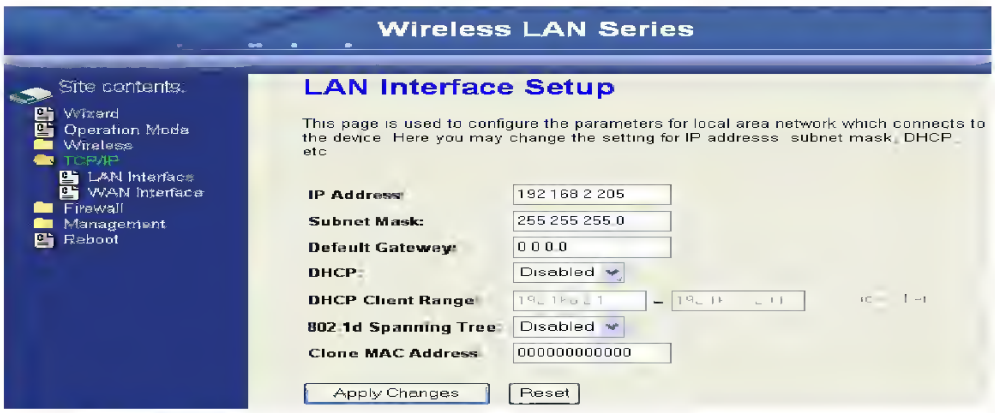


7. Press "Next>>" button then select "None" for "Encryption" then press "Finished" button.

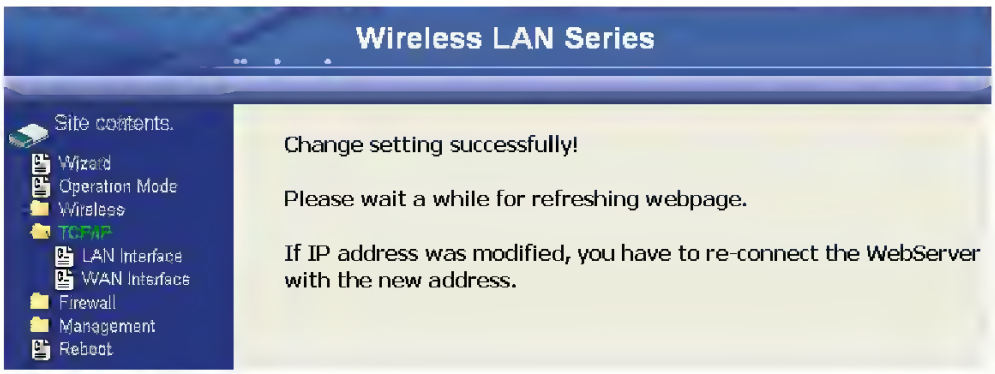
8. Wait for refreshing web page.



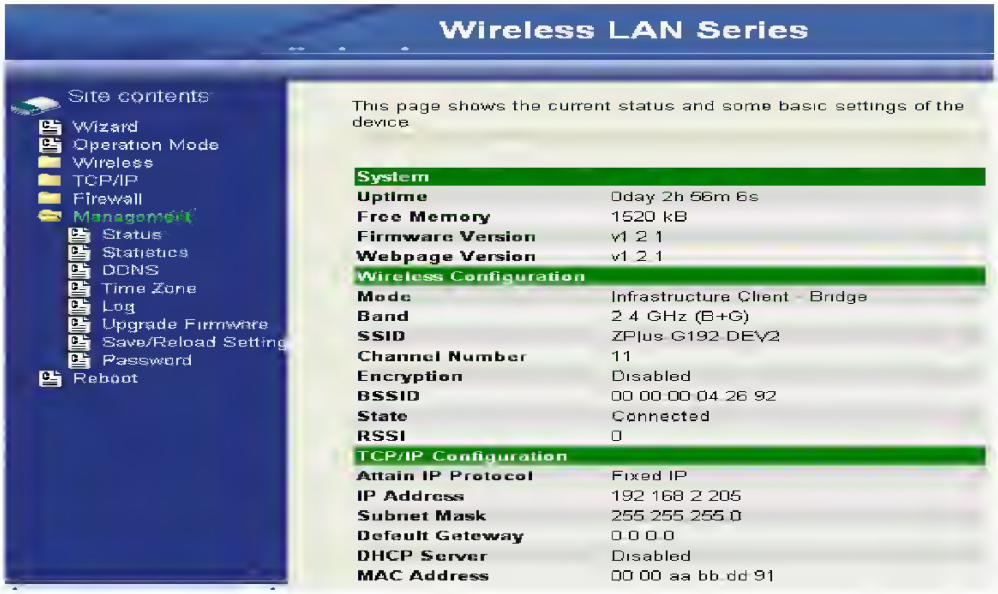
9. Access the web server by the new IP address "192.168.2.205" and use "LAN Interface" page to disable DHCP Server.



10. Wait for refreshing webpage.



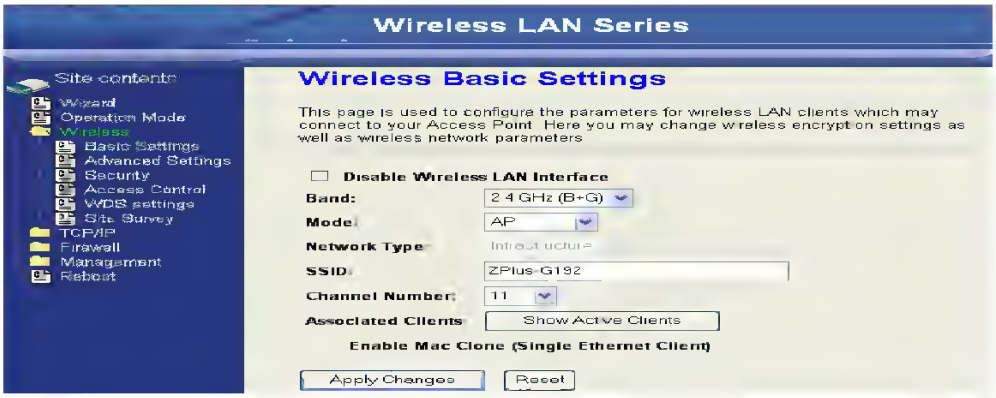
11. Use "State" page to check setting.



12. If the "State" of "Wireless Configuration" is not "Connected" or you want to refresh the "RSSI ", please use "Site Survey" page to re-connect a AP.

Wireless LAN Series
Site contents:
Wizard
Operation Mode
Wireless
Basic Settings
Advanced Settings
Security
Access Control
WDS settings
Site Survey
TCP/IP
Firewall
Management
Reboot
Wireless Site Survey
This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled
SSID BSSID Channel Type Encrypt Signal Select
Mercy_CA_SSID 00:0d:14:00:80:18 9 (B+G) AP no 100
ZPlus-G192 DEV1 00:00:00:04:27:28 11 (B+G) AP no 100
ZPlus-G192 DEV2 00:00:00:04:26:92 11 (B+G) AP no 84
default 00:0f:3d:3d:89:62 6 (B+G) AP no 81
Zinwell 00:05:9e:80:01:f8 1 (B) AP no 80
ZPlus G192 00:aa:ee:ff:99:01 11 (B+G) AP no 63
linksys 00:06:25:d7:c3:67 6 (B+G) AP no 61
ZPlus-G192-mm 00:00:00:04:27:01 2 (B+G) AP no 52
G192-wds2 00:00:00:04:26:93 11 (B+G) AP no 41
DFC-test 00:05:9e:80:46:3b 1 (B) AP no 29
G192-wds1 00:00:00:04:26:88 11 (B+G) AP no 23
SF-PRINTER 00:0c:6e:c1:9b:11 7 (B+G) AP yes 18
Refresh
Connect

Basic Settings



Disable Wireless LAN Interface

Disable the wireless interface of device

Band:

The device supports 2.4GHz(B), 2.4GHz(G) and 2.4GHz(B+G) mixed modes.

Mode:

The radio of device supports different modes as following:

1. AP

   The radio of device acts as an Access Point to serves all wireless clients to join a wireless local network.

2. Client

   Support Infrastructure and Ad-hoc network types to act as a wireless adapter.

3. WDS

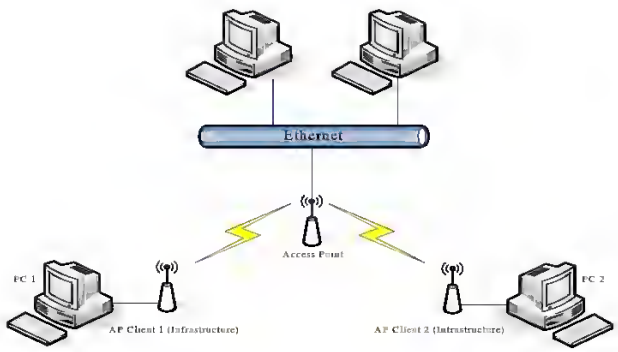
   Wireless Distribution System, this mode serves as a wireless repeater, only devices with WDS function supported can connect to it, all the wireless clients can't survey and connect the device when the mode is selected.

4. AP+WDS

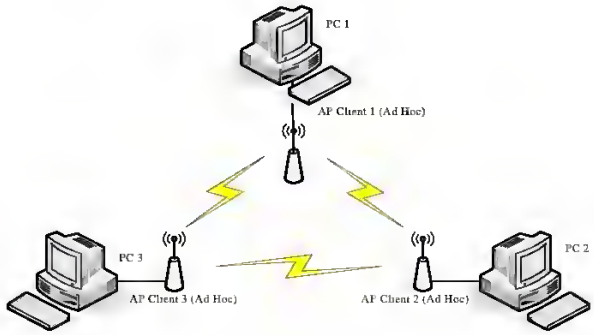
   Support both AP and WDS functions, the wireless clients and devices with WDS function supported can survey and connect to it.

- ***Infrastructure***:

  This type requires the presence of 802.11b/g Access Point. All communication is done via the Access Point.



- ***Ad Hoc***:
  This type provides a peer-to-peer communication between wireless stations. All the communication is done from Client to Client without any Access Point involved. Ad Hoc networking must use the same SSID and channel for establishing the wireless connection.



In client mode, the device can't support the Router mode function include Firewall and WAN settings.

SSID:

The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Multiple access point/bridges on a network or sub-network can use the same SSID. SSIDs are case sensitive and can contain up to 32 alphanumeric characters. Do not include spaces in your SSID.

Channel Number

The following table is the available frequencies (in MHz) for the 2.4-GHz radio:

Channel No.	Frequency	Country Domain
1	2412	Americas, EMEA, Japan, and China
2	2417	Americas, EMEA, Japan, and China
3	2422	Americas, EMEA, Japan, Israel, and China
4	2427	Americas, EMEA, Japan, Israel, and China
5	2432	Americas, EMEA, Japan, Israel, and China
6	2437	Americas, EMEA, Japan, Israel, and China
7	2442	Americas, EMEA, Japan, Israel, and China
8	2447	Americas, EMEA, Japan, Israel, and China
9	2452	Americas, EMEA, Japan, Israel, and China
10	2457	Americas, EMEA, Japan, and China

11	2462	Americas, EMEA, Japan, and China
12	2467	EMEA and Japan only
13	2472	EMEA and Japan only
14	2484	Japan only

When set to “Auto”, the device will find the least-congested channel for use.

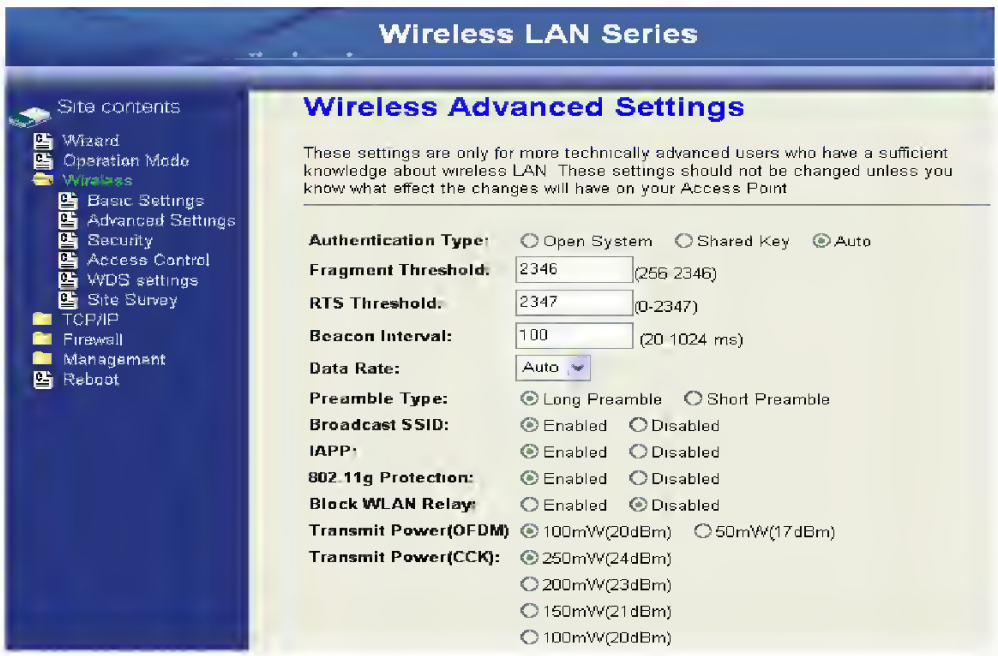
Associated Client

Show the information of active wireless client stations that connected to the device.

Advanced Settings

These settings are only for more technically advanced users who have sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your device. The default setting is optimized for the normal operation. For specific application, setting configuration will required highly attention to reach optimistic condition.

Note : Any unreasonable value change to default setting will reduce the throughput of the device.



Authentication Type

The device supports two Authentication Types “Open system” and “Shared Key”. When you select “Share Key”, you need to setup “WEP” key in “Security” page (See the next section). The default setting is “Auto”. The wireless client can associate with the device by using one of the two types.

Fragment Threshold

The fragmentation threshold determines the size at which packets are fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference. This function will help you to improve the network performance.

RTS Threshold

The RTS threshold determines the packet size at which the radio issues a request to send (RTS) before sending the packet. A low RTS Threshold setting

can be useful in areas where many client devices are associating with the device, or in areas where the clients are far apart and can detect only the device and not each other. You can enter a setting ranging from 0 to 2347 bytes.

Data Rate

The standard IEEE 802.11b/11g supports 1, 2, 5.5,11/6, 9, 12, 18, 24, 36, 48 and Mbps data rates. You can choose the rate that the device uses for data transmission. The default value is "auto". The device will use the highest possible selected transmission rate.

Beacon Interval

The beacon interval is the amount of time between access point beacons in microseconds. The default beacon interval is 100.

Broadcast SSID

Broadcasting the SSID will let your wireless clients find the device automatically. If you are building a public Wireless Network, disable this function can provide better security. Every wireless stations located within the coverage of the device must connect this device by manually configure the SSID in your client settings.

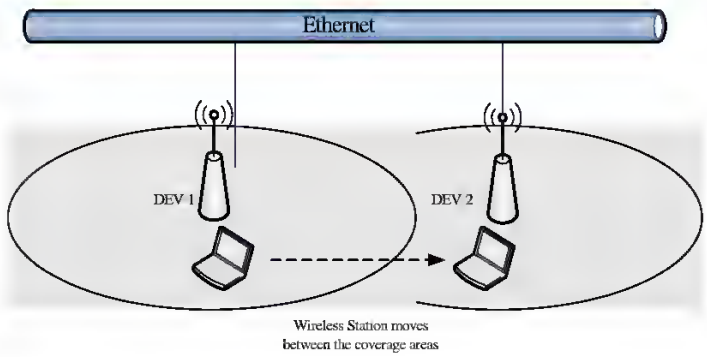
Int. Roaming

This function will let Wireless Stations roam among a network environment with multiple devices. Wireless Stations are able to switch from one device to another as they move between the coverage areas. Users can have more wireless working range. An example as the following figure

You should comply with the following instructions to roam among the wireless coverage areas.

Note : **For implementing the roaming function, the setting MUST comply the following two items.**

- All the devices must be in the same subnet network and the SSID must be the same.
- If you use the 802.1x authentication, you need to have the user profile in these devices for the roaming station.



Block WLAN Relay (Isolate Client)

The device supports isolation function. If you are building a public Wireless Network, enable this function can provide better security. The device will block packets between wireless clients (relay). All the wireless clients connected to the device can't see each other.

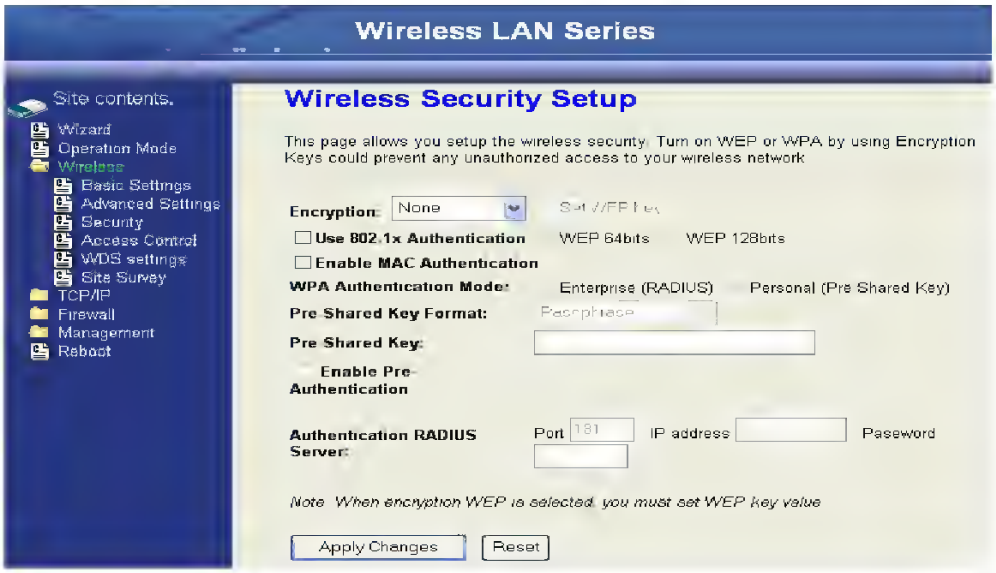
Transmit Power

The device supports four transmission output power levels 250, 200, 150 and 100mW for CCK (802.11b) mode and two transmission output power levels 100 and 50mW for OFDM (802.11g) mode. User can adjust the power level to change the coverage of the device. Every wireless stations located within the coverage of the device also needs to have the high power radio. Otherwise the wireless stations only can survey the device, but can't establish connection with device.

Configuring Wireless Security

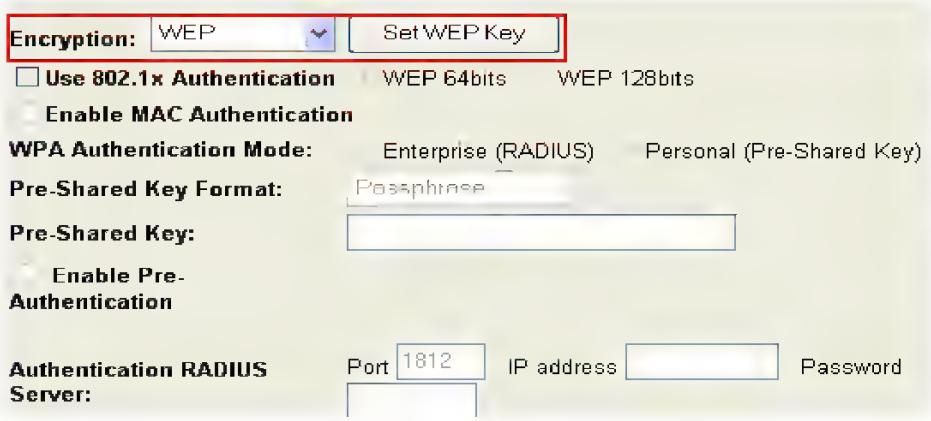
This device provides complete wireless security function include WEP, 802.1x, WPA-TKIP, WPA2-AES and WPA2-Mixed in different mode (see the Security Support Table).

The default security setting of the encryption function is disabled. Choose your preferred security setting depending on what security function you need.



WEP Encryption Setting

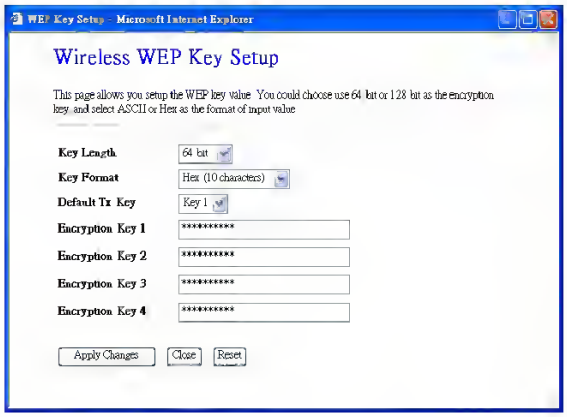
Wired Equivalent Privacy (WEP) is implemented in this device to prevent unauthorized access to your wireless network. The WEP setting must be as same as each client in your wireless network. For more secure data transmission, you can change encryption type to "WEP" and click the "Set WEP Key" button to open the "Wireless WEP Key setup" page.



When you decide to use the WEP encryption to secure your WLAN, please

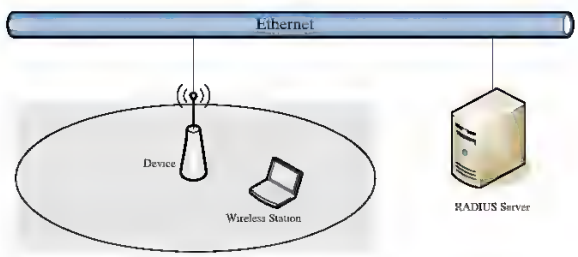
refer to the following setting of the WEP encryption:

- 64-bit WEP Encryption：64-bit WEP keys are as same as the encryption method of 40-bit WEP. You can input 10 hexadecimal digits (0~9, a~f or A~F) or 5 ACSII chars.
- 128-bit WEP Encryption：128-bit WEP keys are as same as the encryption method of 104-bit WEP. You can input 26 hexadecimal digits (0~9, a~f or A~F) or 10 ACSII chars.
- The Default Tx Key field decides which of the four keys you want to use in your WLAN environment.

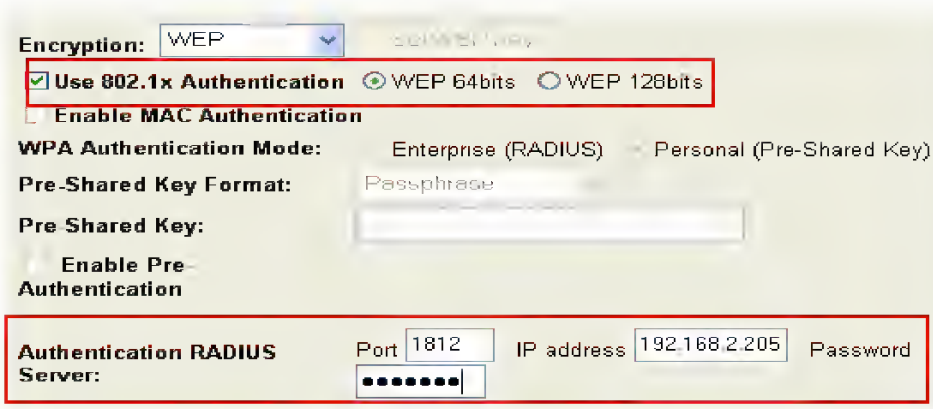

WEP Key Setup - Microsoft Internet Explorer
Wireless WEP Key Setup
This page allows you setup the WEP key value. You could choose use 64-bit or 128-bit as the encryption key, and select ASCII or Hex as the format of input value.
Key Length
64 bit
Key Format
Hex (10 characters)
Default Tx Key
Key 1
Encryption Key 1
Encryption Key 2
Encryption Key 3
Encryption Key 4
Apply Changes
Close
Reset

WEP Encryption with 802.1x Setting

The device supports external RADIUS Server that can secure networks against unauthorized access. If you use the WEP encryption, you can also use the RADIUS server to check the admission of the users. By this way every user must use a valid account before accessing the Wireless LAN and requires a RADIUS or other authentication server on the network. An example is shown as following.



You should choose WEP 64 or 128 bit encryption to fit with your network environment first. Then add user accounts and the target device to the RADIUS server. In the device , you need to specify the IP address、Password (Shared Secret) and Port number of the target RADIUS server.



WPA Encryption Setting

WPA feature provides a high level of assurance for end-users and administrators that their data will remain private and access to their network restricted to authorized users. You can choose the WPA encryption and select the Authentication Mode.

WPA Authentication Mode

This device supports two WPA modes. For personal user, you can use the Pre-shared Key to enhance your security setting. This mode requires only an access point and client station that supports WPA-PSK. For Enterprise, authentication is achieved via WPA RADIUS Server. You need a RADIUS or other authentication server on the network.

- **Enterprise (RADIUS):**

  When WPA Authentication mode is Enterprise (RADIUS), you have to add user accounts and the target device to the RADIUS Server. In the device , you need to specify the IP address、Password (Shared Secret) and Port number of the target RADIUS server.

- **Pre-Share Key:**

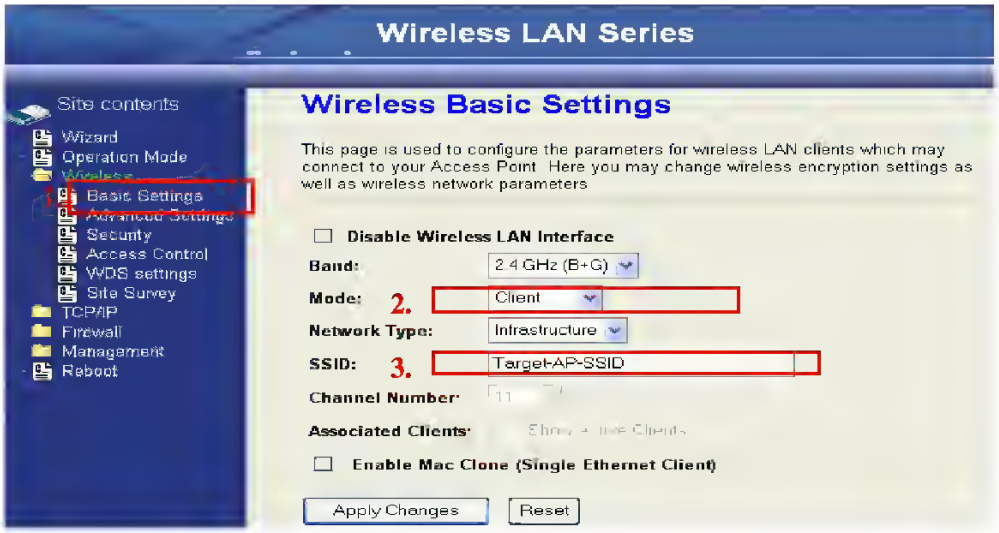
  This mode requires only an access point and client station that supports WPA-PSK. The WPA-PSK settings include Key Format, Length and Value. They must be as same as each wireless client in your wireless network. When Key format is Passphrase, the key value should have 8~63 ACSII chars. When Key format is Hex, the key value should have 64 hexadecimal digits (0~9, a~f or A~F).

Configuring as WLAN Client Adapter

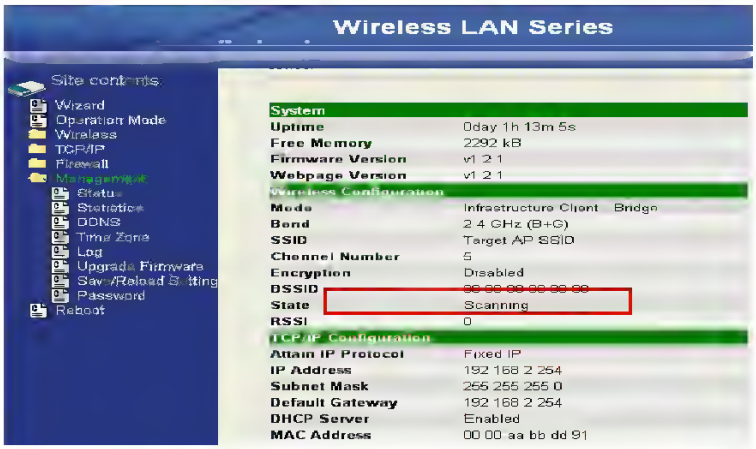
This device can be configured as a wireless Ethernet adapter. In this mode, the device can connect to the other wireless stations (Ad-Hoc network type) or Access Point (Infrastructure network type) and you don't need to install any driver.

Quick start to configure

Step 1. In "Basic Settings" page, change the Mode to "Client" mode. And key in the SSID of the AP you want to connect then press "Apply Changes" button to apply the change.

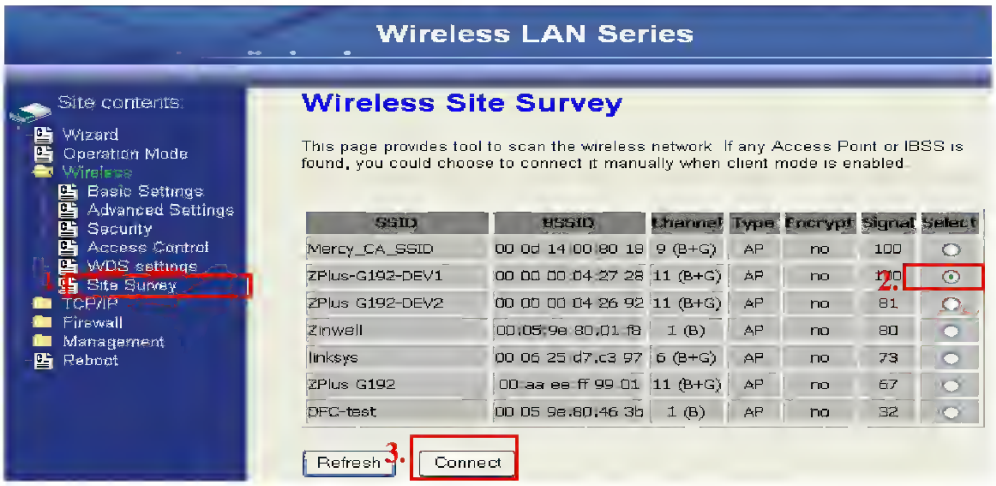


Step 2. Check the status of connection in "Status" web page



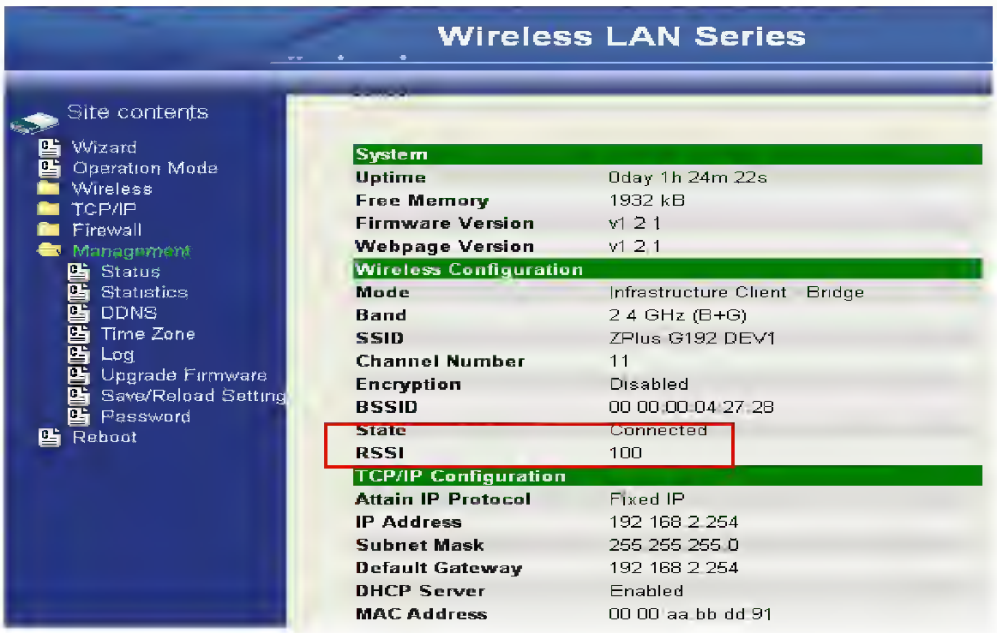
The alternative way to configure as following:

Step 1. In “Wireless Site Survey” page, select one of the SSIDs you want to connect and then press “Connect” button to establish the link.


Wireless LAN Series
Site contents:
Wizard
Operation Mode
Wireless
Basic Settings
Advanced Settings
Security
Access Control
WDS settings
Site Survey
TCP/IP
Firewall
Management
Reboot
Wireless Site Survey
This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.
SSID BSSID Channel Type Encrypt Signal Select
Mercy_CA_SSID 00 0d 14 00 80 18 9 (B+G) AP no 100
ZPlus-G192-DEV1 00 00 00 04 27 28 11 (B+G) AP no 100
ZPlus G192-DEV2 00 00 00 04 26 92 11 (B+G) AP no 81
Zinwell 00 05 9e 80 01 f8 1 (B) AP no 80
linksys 00 06 25 d7 c3 97 6 (B+G) AP no 73
ZPlus G192 00 aa ee ff 99 01 11 (B+G) AP no 67
DFC-test 00 05 9e 80 46 3b 1 (B) AP no 32
Refresh
Connect
1.
2.
3.

Step 2. If the linking is established successfully. It will show the message “Connect successfully”. Then press “OK”.

Step 3. Then you can check the linking information in “Status” page.



Note :

If the available network requires authentication and data encryption, you need to setup the authentication and encryption before step1 and all the settings must be as same as the Access Point or Station. About the detail authentication and data encryption settings, please refer the security section.

Authentication Type

In client mode, the device also supports two Authentication Types "Open system" and "Shared Key". Although the default setting is "Auto", not every Access Points can support "Auto" mode. If the authentication type on the Access Point is knew by user, we suggest to set the authentication type as same as the Access Point.

Data Encryption

In client mode, the device supports WEP and WPA Personal/Enterprise except WPA2 mixed mode data encryption. About the detail data encryption settings, please refer the security section.

Ch 3. Configuring WDS

Wireless Distribution System (WDS) uses wireless media to communicate with the other devices, like the Ethernet does. This function allows one or more remote LANs connect with the local LAN. To do this, you must set these devices in the same channel and set MAC address of other devices you want to communicate with in the WDS AP List and then enable the WDS.

When you decide to use the WDS to extend your WLAN, please refer the following instructions for configuration.

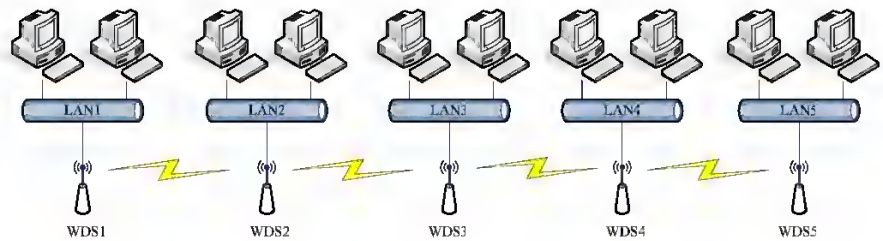
- The bridging devices by WDS must use the same radio channel.
- When the WDS function is enabled, all wireless stations can't connect the device.
- If your network topology has a loop, you need to enable the 802.1d Spanning Tree function.
- You don't need to add all MAC address of devices existed in your network to WDS AP List. WDS AP List only needs to specify the MAC address of devices you need to directly connect to.
- The bandwidth of device is limited, to add more bridging devices will split the more bandwidth to every bridging device.

WDS network topology

In this section, we will demonstrate the WDS network topologies and WDS AP List configuration. You can setup the four kinds of network topologies: bus, star, ring and mesh.

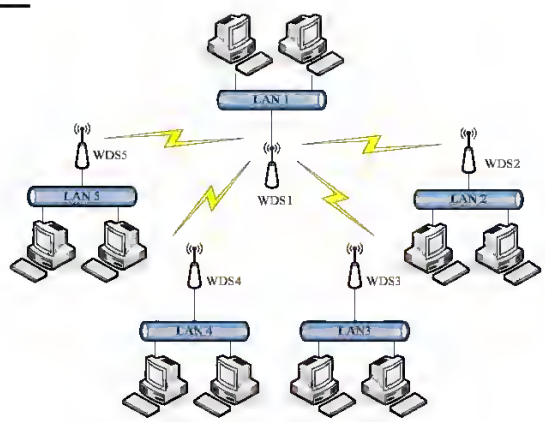
In this case, there are five devices with WDS enabled: WDS1, WDS2, WDS3, WDS4 and WDS5.

Bus topology :



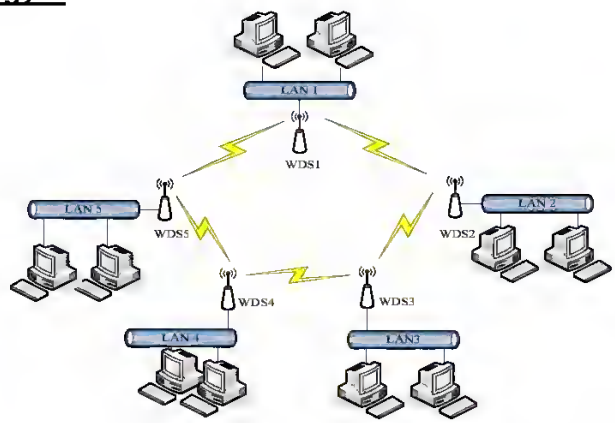
Device	Entries of WDS AP List	Spanning Tree Protocol Required
WDS1	The MAC Address of WDS2	No
WDS2	The MAC Addresses of WDS1 and WDS3	No
WDS3	The MAC Addresses of WDS2 and WDS4	No
WDS4	The MAC Addresses of WDS3 and WDS5	No
WDS5	The MAC Address of WDS4	No

Star topology :



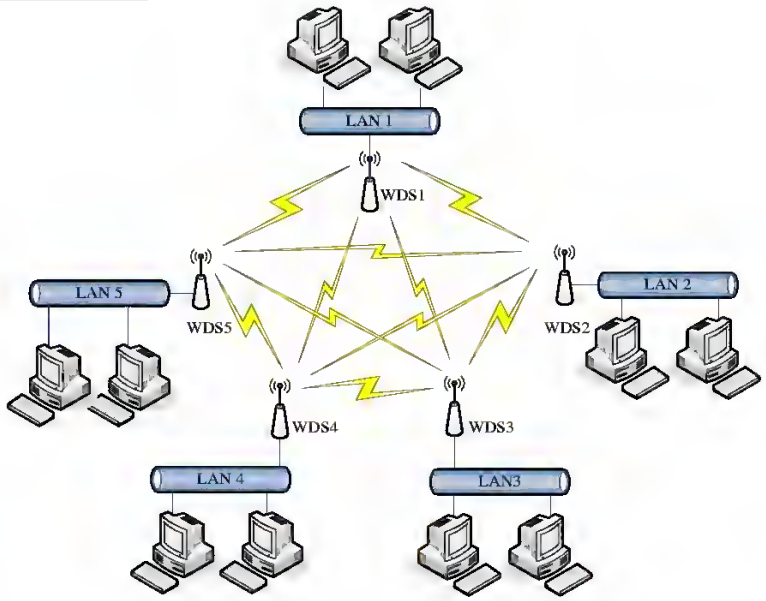
Device	Entries of WDS AP List	Spanning Tree Protocol Required
WDS1	The MAC Addresses of WDS2, WDS3, WDS4 and WDS5	No
WDS2	The MAC Address of WDS1	No
WDS3	The MAC Address of WDS1	No
WDS4	The MAC Address of WDS1	No
WDS5	The MAC Address of WDS1	No

Ring topology :



Device	Entries of WDS AP List	Spanning Tree Protocol Required
WDS1	The MAC Addresses of WDS2 and WDS5	Yes
WDS2	The MAC Addresses of WDS1 and WDS3	Yes
WDS3	The MAC Addresses of WDS2 and WDS4	Yes
WDS4	The MAC Addresses of WDS3 and WDS5	Yes
WDS5	The MAC Addresses of WDS4 and WDS1	Yes

Mesh topology :



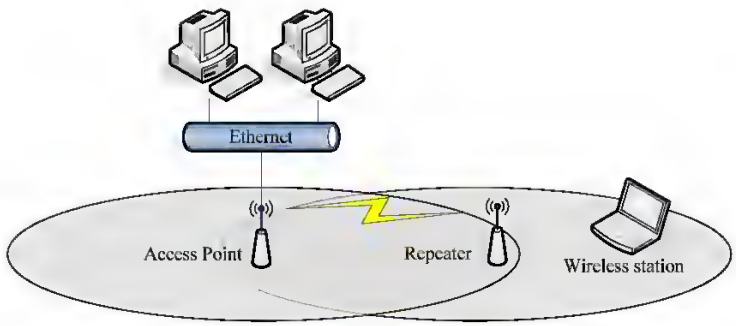
Device	Entries of WDS AP List	Spanning Tree Protocol Required
WDS1	The MAC Addresses of WDS2, WDS3, WDS4 and WDS5	Yes
WDS2	The MAC Addresses of WDS1, WDS3, WDS4 and WDS5	Yes
WDS3	The MAC Addresses of WDS1, WDS2, WDS4 and WDS5	Yes
WDS4	The MAC Addresses of WDS1, WDS2, WDS3 and WDS5	Yes
WDS5	The MAC Addresses of WDS1, WDS2, WDS3 and WDS4	Yes

WDS Application

Wireless Repeater

Wireless Repeater can be used to increase the coverage area of another device (Parent AP). Between the Parent AP and the Wireless Repeater, wireless stations can move among the coverage areas of both devices. When you decide to use the WDS as a Repeater, please refer the following instructions for configuration.

- In AP mode, enable the WDS function.
- You must set these connected devices with the same radio channel and SSID.
- Choose “WDS+AP” mode.
- Using the bus or star network topology.



Description	Entries of WDS AP List	Spanning Tree Protocol Required
Access Point	The MAC Address of Repeater	Yes
Repeater	The MAC Address of Access Point	Yes

Wireless Bridge

Wireless Bridge can establish a wireless connection between two or more Wired LANs. When you decide to use the WDS as a Wireless Bridge, please refer the following instructions for configuration.

- In AP mode, enable the WDS function.
- You must set these connected devices with the same radio channel, but you may use different SSID.
- Choose "WDS" mode for only wireless backbone extension purpose.
- You can use any network topology, please refer the WDS topology section.

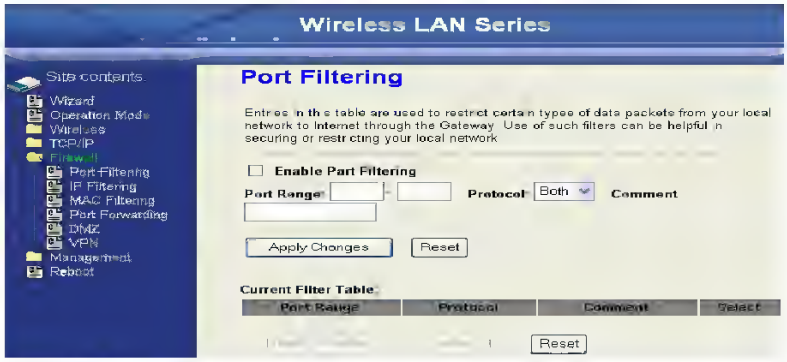
Ch 4. Advanced Configurations

Configuring LAN to WAN Firewall

Filtering function is used to block packets from LAN to WAN. The device supports three kinds of filter Port Filtering, IP Filtering and MAC Filtering. All the entries in current filter table are used to restrict certain types of packets from your local network to through the device. Use of such filters can be helpful in securing or restricting your local network.

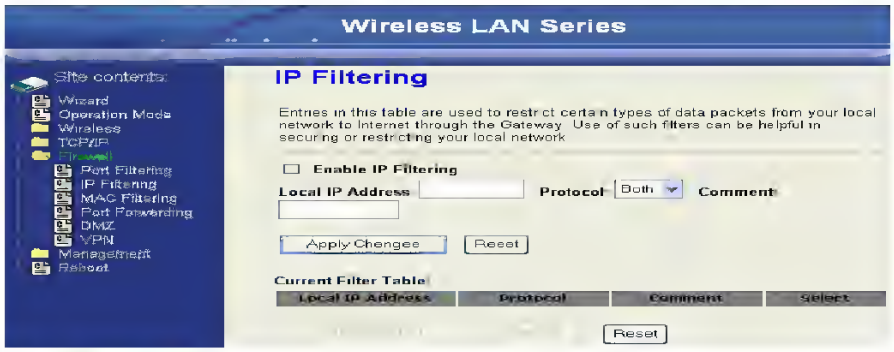
Port Filtering

When you enable the Port Filtering function, you can specify a single port or port ranges in current filter table. Once the source port of outgoing packets match the port definition or within the port ranges in the table, the firewall will block those packets from LAN to WAN.



IP Filtering

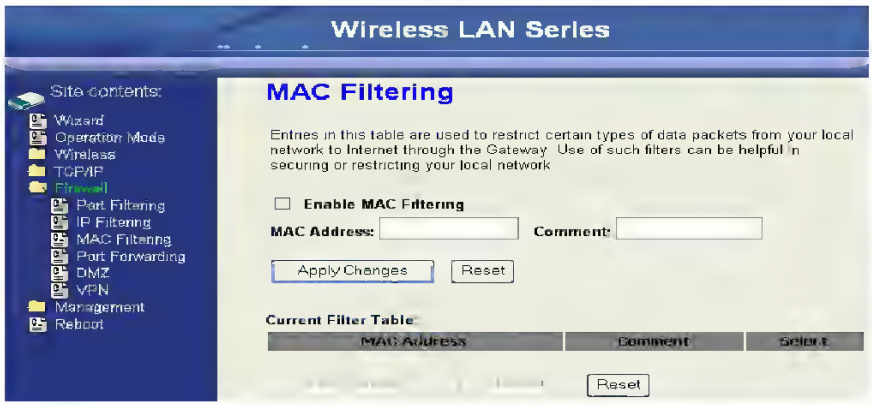
When you enable the IP Filtering function, you can specify local IP Addresses in current filter table. Once the source IP address of outgoing packets match the IP Addresses in the table, the firewall will block this packet from LAN to WAN.



MAC Filtering

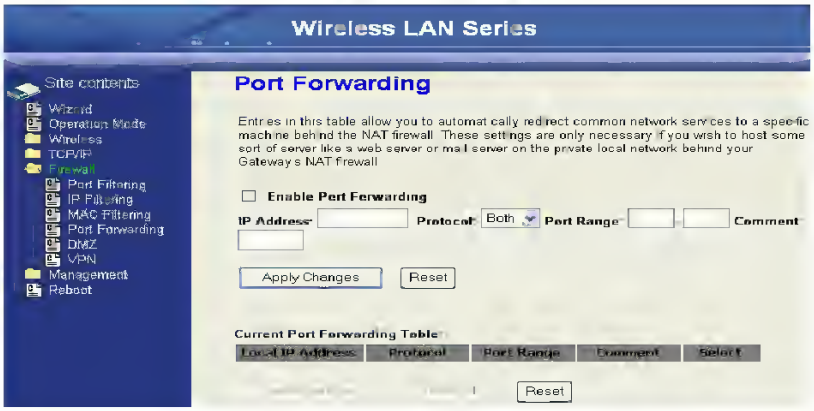
When you enable the MAC Filtering function, you can specify the MAC

Addresses in current filter table. Once the source MAC Address of outgoing packets match the MAC Addresses in the table, the firewall will block this packet from LAN to WAN.



Configuring Port Forwarding (Virtual Server)

This function allows you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind the device's NAT firewall.



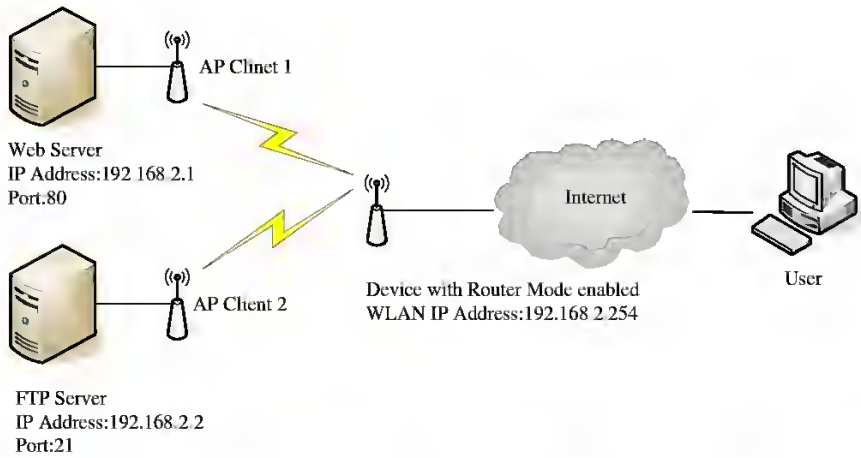
The most often used port numbers are shown in the following table.

Services	Port Number
ECHO	7
FTP (File Transfer Protocol)	21
Telnet	23
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53

Finger	79
HTTP (Hyper Text Transfer Protocol)	80
POP3 (Post Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
SIP (Session Initiation Protocol)	5060
PPTP (Point-to-Point Tunneling Protocol)	1723

Multiple Servers behind NAT Example:

In this case, there are two PCs in the local network accessible for outside users.



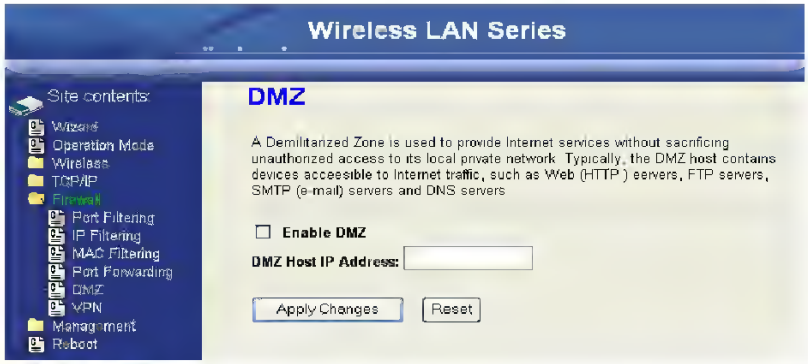
Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select
192.168.2.1	TCP+UDP	80	Web Server	☐
192.168.2.2	TCP+UDP	21	FTP Server	☐

Delete Selected | Delete All | Reset

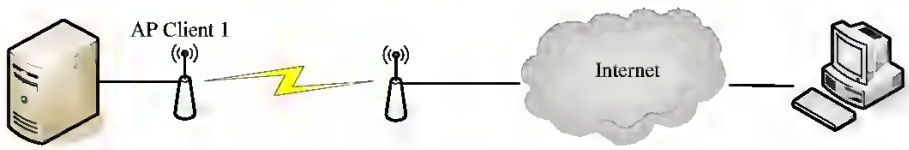
Configuring DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers. So that all inbound packets will be redirected to the computer you set. It also is useful while you run some applications (ex. Internet game) that use uncertain incoming ports.



Enable DMZ: Enable the "Enable DMZ", and then click "Apply Changes" button to save the changes.

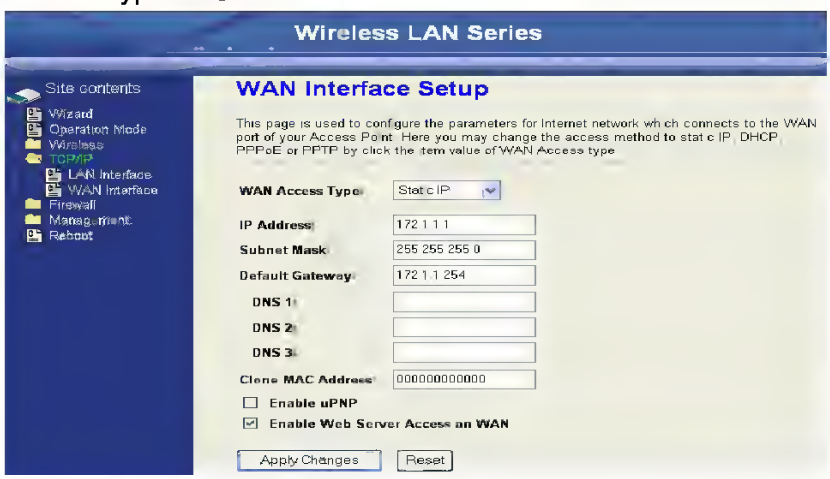
DMZ Host IP Address: Input the IP Address of the computer that you want to expose to Internet.



DNS Host Device with Router Mode enabled

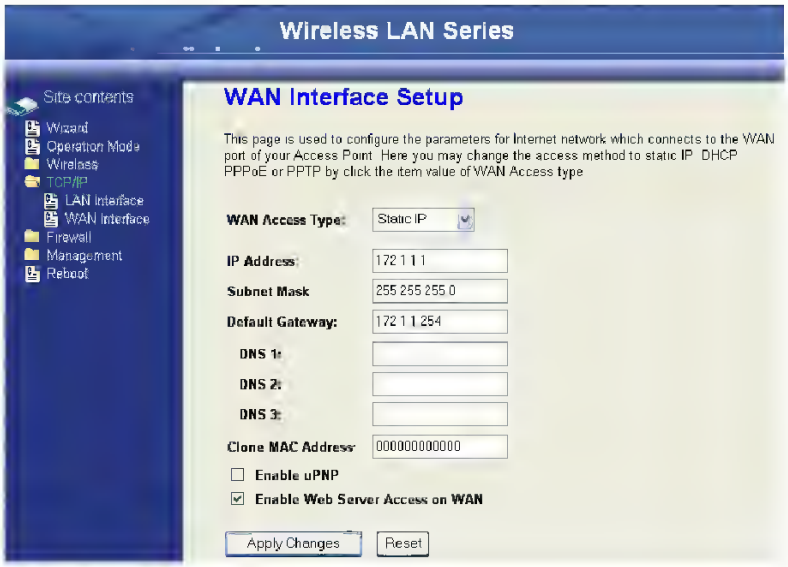
Configuring WAN Interface

The device supports four kinds of IP configuration for WAN interface, including Static IP, DHCP Client, PPPoE and PPTP. You can select one of the WAN Access Types depend on your ISP required. The default WAN Access Type is "Static IP".



Static IP

You can get the IP configuration data of Static-IP from your ISP. And you will need to fill the fields of IP address, subnet mask, gateway address, and one of the DNS addresses.



IP Address: The Internet Protocol (IP) address of WAN interface provided by your ISP or MIS. The address will be your network identifier besides your local network.

Subnet Mask: The number used to identify the IP subnet network, indicating whether the IP address can be recognized on the LAN or if it must be reached through a gateway.

Default Gateway: The IP address of Default Gateway provided by your ISP or MIS. Default Gateway is the intermediate network device that has knowledge of the network IDs of the other networks in the Wide Area Network, so it can forward the packets to other gateways until they are delivered to the one connected to the specified destination.

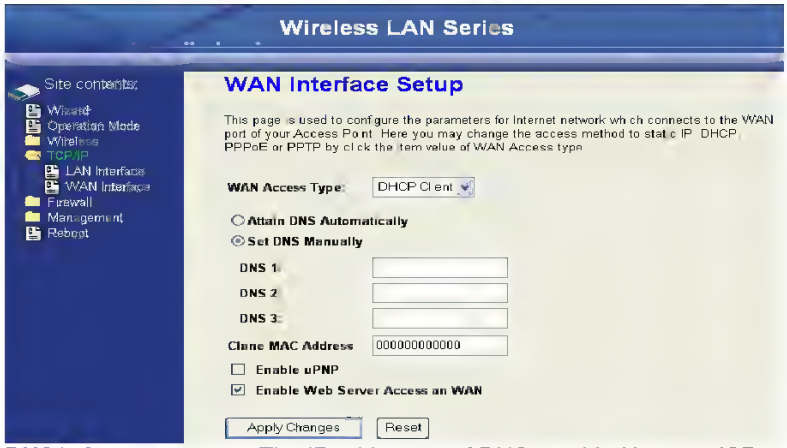
DNS 1~3: The IP addresses of DNS provided by your ISP. DNS (Domain Name Server) is used to map domain names to IP addresses. DNS maintain central lists of domain name/IP addresses and map the domain names in your Internet requests to other servers on the Internet until the specified web site is found.

Clone MAC Address: Clone device MAC address to the specify MAC address required by your ISP

Enable uPnP: Enable uPnP, this function allows the device to be found and configured automatically by the system. (Ex. Window XP)

DHCP Client (Dynamic IP)

All IP configuration data besides DNS will obtain from the DHCP server when DHCP-Client WAN Access Type is selected.


Wireless LAN Series
Site contents:
Wizard
Operation Mode
Wireless
TCP/IP
LAN Interface
WAN Interface
Firewall
Management
Reboot
WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.
WAN Access Type: DHCP Client
Attain DNS Automatically
Set DNS Manually
DNS 1:
DNS 2:
DNS 3:
Clone MAC Address: 000000000000
Enable uPNP
Enable Web Server Access on WAN
Apply Changes
Reset

DNS1~3: The IP addresses of DNS provided by your ISP.

DNS (Domain Name Server) is used to map domain names to IP addresses. DNS maintain central lists of domain name/IP addresses and map the domain names in your Internet requests to other servers on the Internet until the specified web site is found.

Clone MAC Address: Clone device MAC address to the specify MAC address required by your ISP

Enable uPnP: Enable uPnP, this function allows the device to be found and configured automatically by the system. (Ex. Window XP)

PPPoE

When the PPPoE((Point to Point Protocol over Ethernet) WAN Access Type is selected, you must fill the fields of User Name, Password provided by your ISP. The IP configuration will be done when the device successfully authenticates with your ISP.

User Name: The account provided by your ISP

Password: The password for your account.

Connect Type: "Continuous " : connect to ISP permanently

"Manual" : Manual connect/disconnect to ISP

"On-Demand" : Automatically connect to ISP when user need to access the Internet.

Idle Time: The number of inactivity minutes to disconnect from ISP. This setting is only available when "Connect on Demand" connection type is selected.

MTU Size: Maximum Transmission Unit, 1412 is the default setting, you may need to change the MTU for optimal performance with your specific ISP.

DNS1~3: The IP addresses of DNS provided by your ISP.

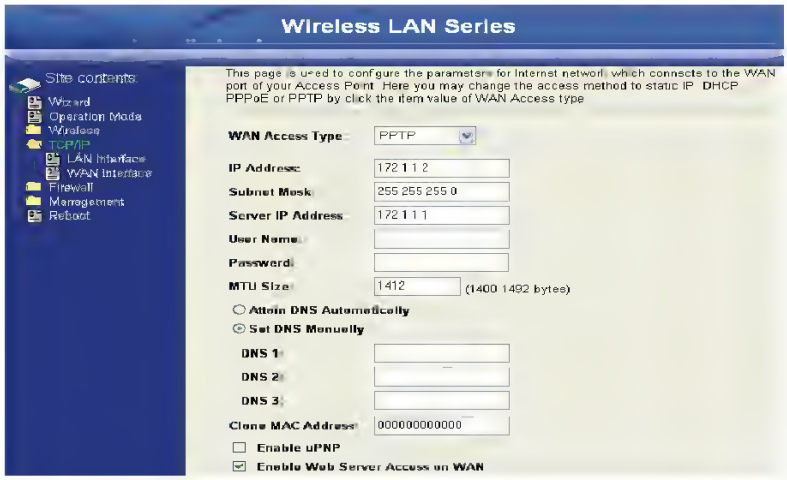
DNS (Domain Name Server) is used to map domain names to IP addresses. DNS maintain central lists of domain name/IP addresses and map the domain names in your Internet requests to other servers on the Internet until the specified web site is found.

Clone MAC Address: Clone device MAC address to the specify MAC address required by your ISP.

Enable UPnP: Enable UPnP, this function allows the device to be found and configured automatically by the system. (Ex. Window XP)

PPTP

Point to Point Tunneling Protocol (PPTP) is a service that applies to connections in Europe only



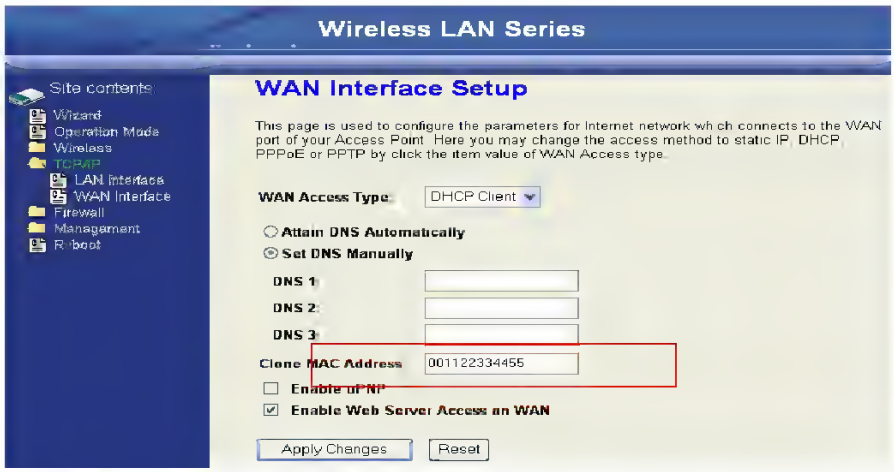
IP Address:	The Internet Protocol (IP) address of WAN interface provided by your ISP or MIS. The address will be your network identifier besides your local network.
Subnet Mask:	The number used to identify the IP subnet network, indicating whether the IP address can be recognized on the LAN or if it must be reached through a gateway.
Server IP Address: (Default Gateway)	The IP address of PPTP server
User Name:	The account provided by your ISP
Password:	The password of your account
MTU Size:	Maximum Transmission Unit, 1412 is the default setting, you may need to change the MTU for optimal performance with your specific ISP.
DNS1~3:	The IP addresses of DNS provided by your ISP. DNS (Domain Name Server) is used to map domain names to IP addresses. DNS maintain central lists of domain name/IP addresses and map the domain names in your Internet requests to other servers on the Internet until the specified web site is found.
Clone MAC Address:	Clone device MAC address to the specify MAC address required by your ISP.
Enable uPnP:	Enable uPnP, this function allows the device to be found and configured automatically by the system. (Ex. Window XP)

Configuring Clone MAC Address

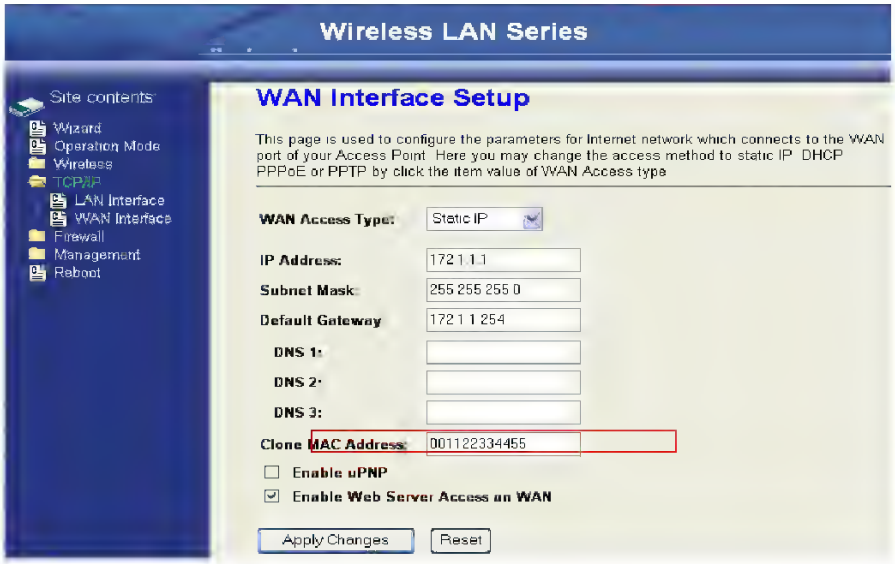
The device provides MAC address clone feature to fit the requirement of some ISP need to specify the client MAC address.

Physical WAN interface MAC Address clone

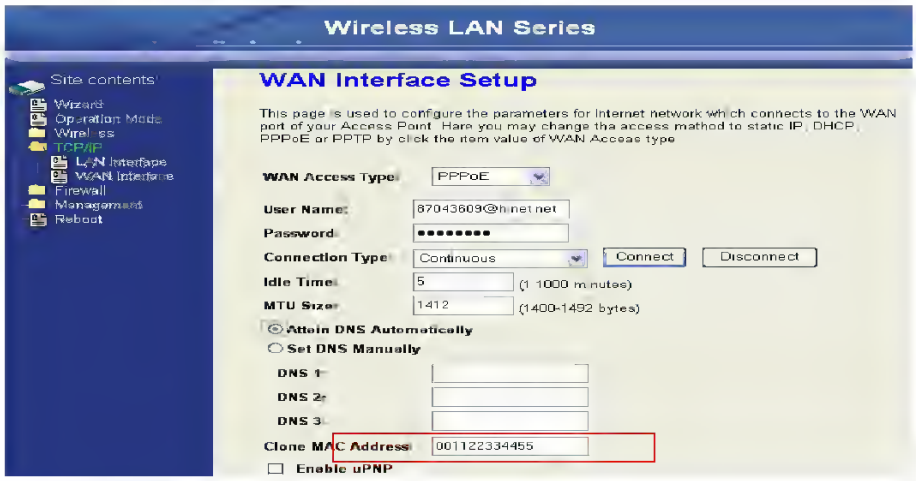
1. Clone MAC address for DHCP Client WAN access type


Wireless LAN Series
Site contents:
Wizard
Operation Mode
Wireless
TCP/IP
LAN Interface
WAN Interface
Firewall
Management
Reboot
WAN Interface Setup
This page is used to configure the parameters for Internet network wh ch connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.
WAN Access Type: DHCP Client
Attain DNS Automatically
Set DNS Manually
DNS 1:
DNS 2:
DNS 3:
Clone MAC Address: 001122334455
Enable uPNP
Enable Web Server Access on WAN
Apply Changes
Reset

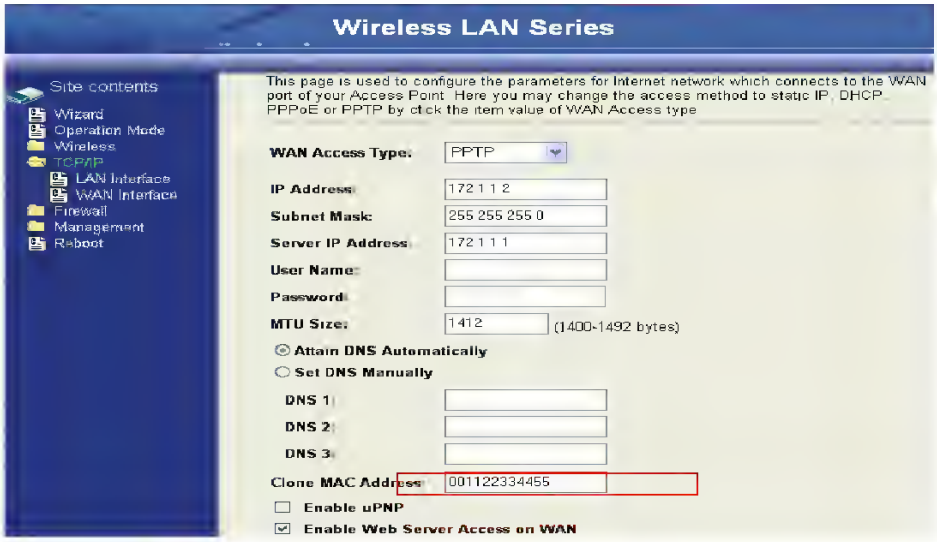
2. Clone MAC address for Static IP WAN access type


Wireless LAN Series
Site contents:
Wizard
Operation Mode
Wireless
TCP/IP
LAN Interface
WAN Interface
Firewall
Management
Reboot
WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.
WAN Access Type: Static IP
IP Address: 172.1.1.1
Subnet Mask: 255.255.255.0
Default Gateway: 172.1.1.254
DNS 1:
DNS 2:
DNS 3:
Clone MAC Address: 001122334455
Enable uPNP
Enable Web Server Access on WAN
Apply Changes
Reset

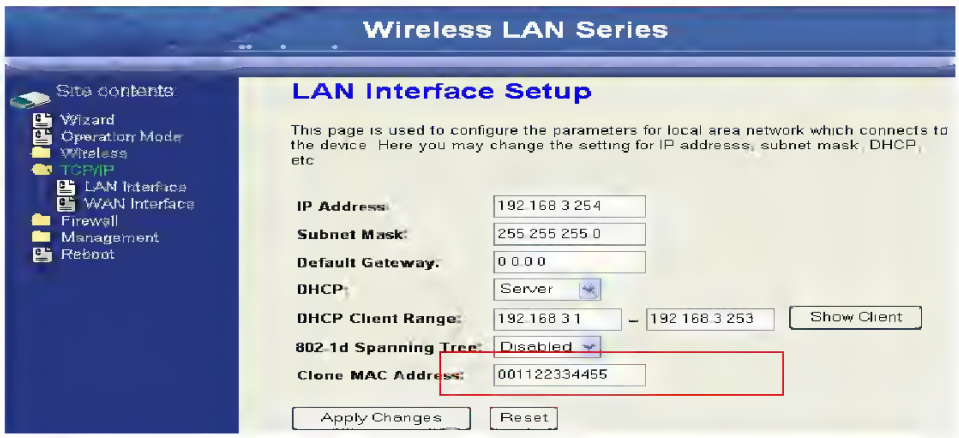
3. Clone MAC address for PPPoE WAN access type



4. Clone MAC address for PPTP WAN access type

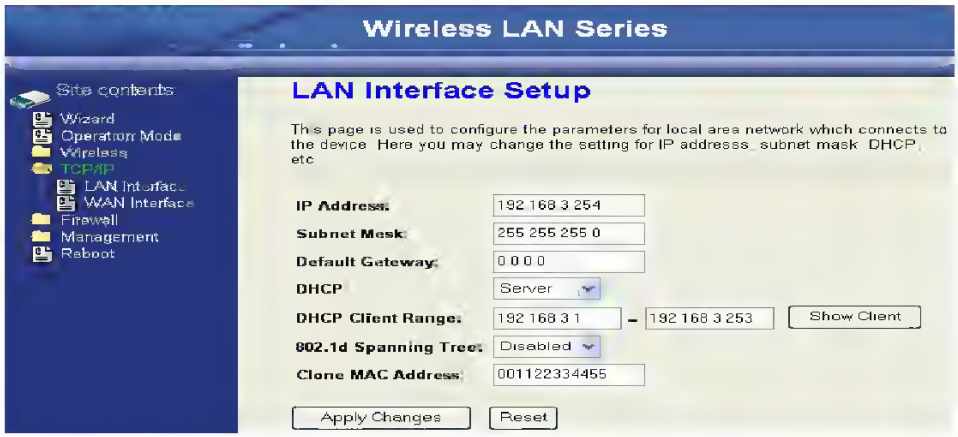


5. Physical LAN interface MAC address clone



Configuring DHCP Server

1. To use the DHCP server inside the device, please make sure there is no other DHCP server existed in the same network as the device.
2. Enable the DHCP Server option and assign the client range of IP addresses as following page.



3. When the DHCP server is enabled and also the device router mode is enabled then the default gateway for all the DHCP client hosts will set to the IP address of device.

Using CLI Menu

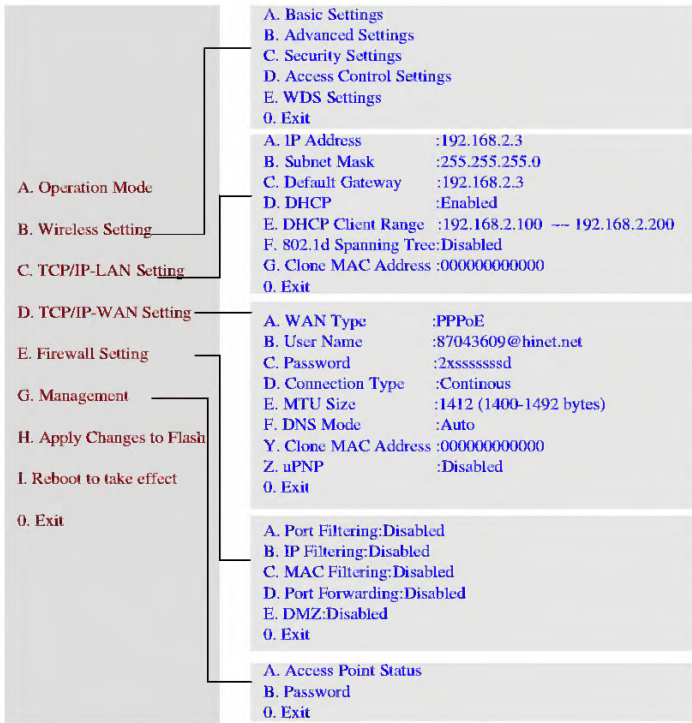
Start a SSH(Secure Shell) client session to login the device

The SSH server daemon inside device uses well-known TCP port 22. User must use SSH client utility such like Putty to login the device. The default password for user "root" is "qwert", once user login the device then can change the password by CLI command.

Execute CLI program

This program won't execute automatically when user login the device. User must manually execute it by typing the case-sensitive command "cli". Please note that any modified settings won't save permanently until user "Apply Changes to Flash" or reboot it. The new settings modified by CLI will take effect after rebooting the device.

Menu Tree List

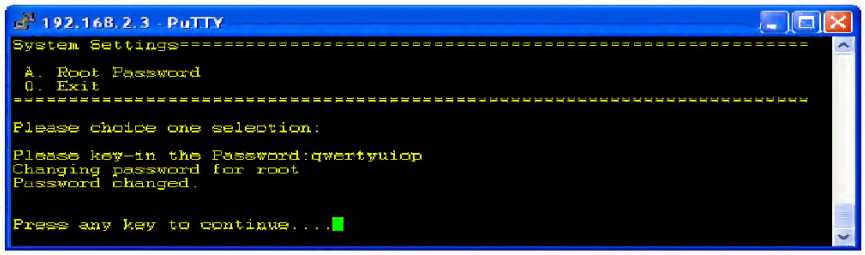

A. Operation Mode
B. Wireless Setting
C. TCP/IP-LAN Setting
D. TCP/IP-WAN Setting
E. Firewall Setting
G. Management
H. Apply Changes to Flash
I. Reboot to take effect
0. Exit
A. Basic Settings
B. Advanced Settings
C. Security Settings
D. Access Control Settings
E. WDS Settings
0. Exit
A. IP Address :192.168.2.3
B. Subnet Mask :255.255.255.0
C. Default Gateway :192.168.2.3
D. DHCP :Enabled
E. DHCP Client Range :192.168.2.100 -- 192.168.2.200
F. 802.1d Spanning Tree:Disabled
G. Clone MAC Address :000000000000
0. Exit
A. WAN Type :PPPoE
B. User Name :87043609@hinet.net
C. Password :2xssssssd
D. Connection Type :Continous
E. MTU Size :1412 (1400-1492 bytes)
F. DNS Mode :Auto
Y. Clone MAC Address :000000000000
Z. uPNP :Disabled
0. Exit
A. Port Filtering:Disabled
B. IP Filtering:Disabled
C. MAC Filtering:Disabled
D. Port Forwarding:Disabled
E. DMZ:Disabled
0. Exit
A. Access Point Status
B. Password
0. Exit

The System Management

Password Protection

Both Web-Browser and SSH configuration interfaces have password protection.

To disable the Web-Browser password protection just leave the "User Name" field to blank then click "Apply Changes" button.



To change the password of user "root" for SSH session, please use the CLI menu item G. System Setting→A. Root Password

About SNMP Agent

This device is compatible with SNMP v1/v2c and provide standard MIB II. Currently only the "public" community string is available and the modified settings by SNMP SET request will be lost after rebooting the device.

Firmware Upgrade

Firmware Types

The firmware for this device is divided into 2 parts, one is web pages firmware the other is application firmware, and the naming usually are g192webpage.bin and g192linux.bin. To upgrade firmware, we suggest user first upgrade the application firmware then web pages firmware.

Upgrading Firmware

The Web-Browser upgrading interface is the simplest and safest way for user, it will check the firmware checksum and signature, and the

wrong firmware won't be accepted. After upgrading, the device will reboot and please note that depends on the version of firmware, the upgrading may cause the device configuration to be restored to the factory default setting, and the original configuration data will be lost! To upgrade firmware, just assign the file name with full path then click "Upload" button as the following page.

Memory Limitation

To make sure the device have enough memory to upload firmware, the system will check the capacity of free memory, if the device lack of memory to upload firmware, please temporarily turn-off some functions then reboot the device to get enough memory for firmware uploading.

Configuration Data Backup & Restore

Rest Setting to Factory Default Value

Since the device is designed for outdoor used, there is no interface outside the housing to reset the configuration value to the factory default value. The device provides the Web-Browser interface to rest the configuration data. After resetting it, the current configuration data will be lost and restored to factory default value.

Saving & Restoring Configuration Data

To save & restore configuration data of device, just assign the target filename with full path at your local host, then you can backup configuration data to local host or restore configuration data to the device.